Accountability & Sanctions for Personal Data Misuse: Position Paper

Introduction

1. Biomedical and health research needs to be trustworthy if it is to retain the support of the public and research participants. There is no evidence of harms arising from breaches of data within the UK academic community to date.[1] However, within a broader context of societal concerns about hacking, data breaches and increasing awareness about the use, linkage and potential misuse of 'big data', academia cannot be complacent about the potential consequences of data breaches from within the research community.[2]

2. The legal frameworks relevant to the use of data are complex, but researchers also have duties, over and above those required by law, to protect and manage data in ethically sound ways. Academic uses of data for research must be protected by robust governance with safeguards, clear lines of accountability and low tolerance for the misuse of data. It is imperative this is achieved without creating an overly risk averse culture that inhibits the legitimate use of data.[3]

3. A recent EAGDA evidence-gathering exercise summarised the legislative, regulatory and policy framework around sanctions for personal data misuse[4]. It found a lack of consistency in approaches to handling instances of data misuse across funders and other organisations with authority and oversight of researcher behaviour. This is apparent both for the types of events that might trigger sanctions and the types and severity of actions that might be taken.

Analysis

4. Sanctions for data misuse can be punitive when an instance of misuse has occurred and also act as a deterrent against it. They can also demonstrate to the public, data producers and other data users that researchers are accountable for their actions. This may be particularly important where data sharing is not the norm and relationships of trust have not yet been firmly established.

5. Funders' sanctions need to be coherent, clearly communicated, and feasible to enforce. Where breaches fall under the jurisdiction of legal frameworks such as data protection law, funder sanctions need to align with these and follow from the legal process. Where breaches or inappropriate actions relate more to ethical or scientific principles, funder sanctions should be coherent and proportionate to the nature of the offence.

---

[1] Nuffield Council on Bioethics report, co-commissioned by EAGDA: http://nuffieldbioethics.org/wp-content/uploads/A-Review-of-Evidence-Relating-to-Harms-Resulting-from-Uses-of-Health-and-Biomedical-Data-FINAL.pdf

[2] See the Wellcome Trust's evidence to the Health Select Committee on the impact on research from the suspension of access to data from HSCIC in 2014-15 as a result of the fallout from *care.data*: [Accessed 08 April 2016] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/written/18669.html

[3] The rationale for this work developed from EAGDA's 2013 statement on re-identification, which stated that in cases of malicious breaches of research data security *"it should be made clear as a matter of best practice that there are legal as well as scientific penalties for breaching the privacy of participants"* (Recommendation 9) and *"it is funders' responsibility to provide clear notice of the sanctions process, including a statement of who will make these judgements and on what evidence, together with a transparent appeals process"* (Rec. 10)

[4] See accompanying paper: "Sanctions for Data Misuse: Evidence Paper"

6. However, if action is only taken at the point where a breach is identified, there are limited opportunities to make fixes or improvements that would mitigate future risks. The majority of data breaches are accidental, caused by human error or flawed systems of data security and management. There may also be inadvertent procedural breaches that do not lead to subsequent data breaches.

7. Solely punitive measures, whether addressed at researchers or institutions, are not likely to address these underlying factors. Heavy-handed responses to procedural failures or errors will also not help encourage a culture of good practice and learning over time.

8. Many instances of misuse could be avoided or mitigated by encouraging the development of good practice in data governance and data handling, learning from mistakes and investing in data use training and infrastructures. Funders are well placed to motivate researchers towards better data security, management and curation practices.

9. Proactive policies aimed at promoting research integrity and good practice target the poor processes, and/or the circumventing of established processes, that create a risk of data misuse before incidents of misuse actually occur. These seek to improve research practice and accountability as part of a broader governance framework, shifting towards a culture of responsibility for research practice rather than minimal compliance[5].

10. Tools such as auditing and mandatory staff training could be supported by funders as part of a systematic approach to improving and incentivising good data practice. These should be calibrated to risks and not overly burdensome.

11. Existing resources such as the IG Toolkit could be promoted as key tools for good data management. Lessons could be learned from other sectors, for example, a 'Health and Safety Executive' approach to ensuring compliance, or the approach taken by the Civil Aviation Authority which requires mandatory reporting of incidents. Extensive technical solutions could be deployed to ensure research data is appropriately accessed, such as through innovations in digital rights management systems.

12. Accredited researcher training or approved codes of conduct reflect a holistic and harmonised approach to best practice. Training developed by the UK Data Service could be a useful model to adapt and disseminate across other fields of research, providing clear motivations for researchers to undertake training that will likely reduce the risk of inadvertent data breaches.

13. The actions and behaviours covered by a holistic regime of sanctions and proactive policies sit along a spectrum, from illegal actions to poor research and data security practice, and from there to good research practice including enabling access to data where appropriate. There would be strong benefits to considering this approach in the context of funders' other efforts and initiatives to promote good practice, as part of a broader governance framework that drives researchers towards better data use, security and management overall.

[5] For example, the GA4GH accountability policy is designed specifically for genomic research but the principles it upholds could be widely applicable to other research fields.

Recommendations

Funders have an opportunity to frame sanctions for data misuse within a broader drive towards motivating better, more consistent research practice for data use. Ensuring good practice for the use and management of data cannot, however, be achieved by funders alone: data repositories, universities, research institutions, consortia, learned societies, data controllers and publishers all have a stake in providing accountability.

EAGDA recommends that funders should:

1. Work with other stakeholders including universities and data repositories to develop a coherent and proportionate sanctions regime for data use and management. This should address the whole spectrum from legal breaches of data protection law through to failures to adhere to ethical standards of data practice.
2. Work with other stakeholders including universities and data repositories to embed this sanctions regime within a broader spectrum of actions to support and enhance good practice.
3. Build on the sanctions and tools for promoting good practice articulated in existing data governance policies and seek to ensure consistency with these as far as possible.
4. Extend the concept of ‘poor research practice’ to include failure to enable access to data where appropriate.
5. Develop a coherent set of messages for the research community about:
    a. The importance of good practice in data use and management
    b. The measures that stakeholders will use to uphold good standards and how they will act on evidence of non-compliance.
6. Consider explicitly including training costs on data security, curation and management in grant funding with an expectation that all researchers using data will be trained in accordance with standards of best practice for their field.