

GOVERNMENT SOCIAL RESEARCH UNIT

Contact

Email:

15.02.08

Government Social Research Unit response to Data Sharing Review

The response below is a result of consultation with the Heads of Profession for the Government Social Research community (GSR) within Whitehall departments and the devolved administrations. As it is difficult to adequately represent all of the different data sharing issues across GSR our response covers high-level, general data sharing issues only.

Further detail on specific departmental data sharing issues will be covered in responses from individual departments.

Please note, we have read and agree with the issues and concerns raised by the Office of National Statistics (ONS) in their response to this consultation and support their views.

1. Background

The Government Social Research Unit (GSRU) is the professional body for social researchers in government. The GSR community collects, holds and shares personal information in order to support policy formulation, delivery and evaluation. Government Social Researchers are employed in a wide range of government departments, agencies and the devolved administrations and as a result work with data from a very wide spectrum of sources and policy areas.

2. Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Sharing personal data can avoid the need for multiple data gathering exercises thus resulting in efficiencies in both time and cost. It also reduces burden on both individuals and organisations by ensuring that data is collected once but used many times. The opportunity to use data from a variety of sources allows analysts to provide a more complete and accurate picture of an issue which in turn produces better, more robust evidence on which to base policy decisions. The linking of individual records also allows

exploration of more complex issues and relationships. The ability to combine data from many areas supports the development of more sophisticated cross-cutting performance measures to be developed and monitored.

A key risk is the possibility of data leakage due to insufficient data sharing/security processes and protocols. There are also risks to society in terms of data quality and inaccuracy - any errors in data are likely to be reproduced and exacerbated by sharing, necessitating careful and thorough quality assurance? procedures.

The sharing of personal data across government departments and other public bodies would be beneficial for the development of cross-government indicators and also for advancing understanding of some of the larger social science issues, for example climate change and migration. Some sharing is currently taking place but this is limited due to current legal requirements in addition to ethical scrutiny processes and concerns about public acceptability.

3. The legal framework

One of the areas of current procedure that has an impact on social research is the DH Research Governance Framework. The NHS Research Ethics Committee scrutinises all research using NHS clients/facilities and assesses the data sharing/linking proposed for each project. This can have a negative impact if the members of the committee do not have sufficient knowledge or understanding of the Data Protection Act and social research as a discipline. Work is ongoing to improve the knowledge of committee members in relation to the social sciences and DH is also in the process of setting up a Social Care Research Ethics Committee.

4. Consent and transparency

The extent to which the need for individuals consent is required is not always clear and depends on the type of data and the circumstances under which it is to be shared. In terms of social research GSR have published 'Professional Guidance on ethical assurance' which sets out the key principles which should be upheld in the conduct of social research for government, including ensuring participation is based on valid informed consent. Admin data and monitoring data are not covered by this guidance.

A requirement for gaining consent would be particularly problematic for retrospectively gaining explicit consent to share administrative data as this would be both very difficult and costly. This is especially an issue when administrative data is being used to draw potential samples of respondents who will then be given full opportunity to opt-out of a survey later on.

5. Technology

It is difficult to give a cross-GSR view on this, but in general it could be argued that an increase in technological advances has meant more ways of accessing data which in turn can lead to an increase in risk.

Many departments are now moving towards a general rule that no data (disclosive or non-disclosive) should be held on portable devices etc. this applies to both government employees and contractors.

If you have any queries or require any further information please do not hesitate to contact me.

Government Social Research Unit