Trust, Security and Public Interest: Striking the Balance

A review of previous literature on public attitudes towards the sharing, linking and use of administrative data for research

Elizabeth Waind

Administrative Data Research UK (ADR UK) Strategic Hub, elizabeth.waind@ukri.org

Abstract

This literature review explores previous work in relation to the UK public’s attitudes towards the sharing, linking and use of administrative data for research. It finds the public is broadly supportive of administrative data research if three core conditions are met: public interest, privacy and security, and trust and transparency. None of these three conditions is sufficient in isolation; the literature shows public support is underpinned by fulfillment of all three. However, it also shows that in certain cases where the standard of one condition is very high – particularly public interest – this could mean that of another may, if necessary, be lower. An appropriate balance must be struck, and the proposed benefit must outweigh the potential risk.

Broad, conditional support for the use of administrative data in research has not only been found consistently but has also been held over time. However, little previous work – with the exception of that in relation to medical research – has focused on gaining input from relevant demographics and communities on how their data should be used to address specific issues relevant to them. Future work should therefore aim to build upon existing knowledge of broader public attitudes by delving into specific areas of research, not to consult on whether research using administrative data should be done – as has been the focus of previous literature – but to guide how, why and when it is done. Nevertheless, it is important to continue to monitor and respond to any changes to broader public attitudes.

Keywords – public attitudes; public views; public engagement; literature review; administrative data research

1 Introduction

Across the UK, administrative data – information created when people interact with public services such as schools and the National Health Service (NHS) – is a largely untapped but information-rich resource for research. When analysed, this wealth of data has the potential to provide valuable insights into society and highlight where change is needed to improve policy and service provision. The UK government’s 2017 Digital Economy Act (1) provides the legal framework for public authorities to share administrative data for research under Section 64 – ‘Disclosure of information research for purposes’. This allows investments such as ADR UK (Administrative Data Research UK) – a programme funded by the Economic & Social Research Council (ESRC) with a mission to enable secure access to UK public sector administrative data for research in the public interest – to operate.

However, in addition to operating in line with this legal framework, it is essential those handling and using data operate openly and ethically, and in the knowledge the public is supportive of how and why their data is used. Administrative data includes all those who interact with public services and therefore most of the population; that’s what makes it so valuable to understanding society. If we are to use data about the public, this cannot be done without their support and, where possible, their input.

1.1 Objectives

This literature review has the following main objectives:

1. To explore public attitudes, as found by previous research, towards the sharing, linking and use of administrative data for research and the conditions under which it should and should not happen;

2. To be a source of advice on approaches to public engagement for organisations and researchers working with administrative data.

1.2 Definitions

For the purpose of this review, the following key terms are defined:

Anonymised data, as defined by the UK Information Commissioner’s Office (ICO) (2), refers to ‘data in a form that does not identify individuals and where identification through its combination with other data is
not likely to take place’ (p.48). In addition to de-identification (see below), safeguards such as the ‘Five Safes’ – Safe people, Safe projects, Safe settings, Safe outputs and Safe data (3) – provide the conditions under which identification is not likely to take place.

De-identified data refers to data which has had all personal identifying elements such as names and addresses removed. The UK Digital Economy Act Research Code of Practice and Accreditation Criteria (4) states: ‘Data must be de-identified before they can be made available so that the data do not directly identify individuals and are not reasonably likely to lead to an individual’s identity being ascertained’.

It is important to note both ‘de-identified’ and ‘anonymised’ data are referred to in the literature reviewed, with definitions not consistently provided. This does not detract from the fundamental findings of this review; however, when the terms are used in the context of a previous study’s findings, their precise definitions should be considered with some caution.

Personal data, as defined by the European Union General Data Protection Regulation (GDPR) (and referred to by the ICO) (5), is ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’

Public engagement, as defined by Gene Rowe and Lynn J. Frewer in their 2005 ‘A typology of public engagement mechanisms’ (6), is a combination of three concepts: ‘public communication’ (a one-way flow of information to the public); ‘public consultation’ (in which the opinions of the public are sought, but no dialogue is involved) and ‘public participation’ (an exchange of information between the public and those leading the initiative in question).

Transparency, as defined by the ICO (7) in the context of the GDPR, is ‘about being clear, open and honest with people from the start about who you are, and how and why you use their personal data’.

2 Methods

To meet the above objectives, a review of previous public consultations and attitudinal studies conducted in the UK on the topic was completed. These include mostly independent publications by data infrastructures, research institutions or public bodies, as well as academic research papers and existing reviews of previous research. This is not a systematic review; it is a narrative review of the main themes identified across previous work.

In total, 16 papers are included in the review, for which data was collected between 2006-2018, therefore covering over a decade of recent research. The studies were identified via an unsystematic online search without fixed search terms, which included broad searches using internet search engines and browsing the websites of relevant data infrastructures or social research organisations. As this is an unsystematic review and most relevant papers are independently published by organisations rather than in academic publications, and are therefore not always included in databases, an unsystematic approach was the most effective way of identifying relevant literature.

Only papers relevant to public attitudes towards the sharing and use of public sector administrative data for research were selected. Some of the studies reviewed cover attitudes to data use more generally, not only in relation to research, but are nevertheless relevant to the aims of this review. Literature not considered relevant and therefore not reviewed includes papers focused solely on commercial access to data; papers concerned with the linking of public sector data to private sector data; and those focused more broadly on the public’s knowledge of, but not attitudes towards, the collection and storage (and not necessarily use) of data.

3 Overview of existing literature

Previous work has largely focused on the acceptability of data sharing and use amongst the general public, exploring the conditions under which sharing and use is broadly acceptable and therefore offering insight into appropriate approaches for data infrastructures and researchers in general.

However, with the exception of studies focused around the use of health data, there has been little previous literature that has sought the views of particular communities and demographics on the use of their data in specific areas of research relevant to them. The primary focus of existing literature has therefore been to consult on whether research using administrative data should be done, with little input sought from the public on how, why and when it should done in the context of specific programmes of research.

4 Existing public knowledge of administrative data research

In general, the literature reviewed has found that existing public knowledge of how administrative data is currently shared and used by the public sector is low, and that this
can have an impact on levels of support for research using administrative data.

Study participants have been found to assume data is already linked and shared across government and have been surprised to hear it is not more widely used, deeming this to be wasteful (8, 9, 10). Study participants have also expressed confusion between the use of data for research as opposed to for the everyday operation or activities of a public body or service (9, 10).

Most participants of the public consultation, ‘Dialogue on Data: Exploring the public’s views on using administrative data for research purposes’ – conducted by Ipsos MORI on behalf of the ESRC to inform the work of the Administrative Data Research Network (ADRN), the predecessor to ADR UK – (9) attached some value to social research more broadly, though some initially questioned it and compared research findings to ‘common sense’ (p.2). As knowledge increased over the course of the consultation, as did support for administrative data research. This is reflected in numerous other studies (8, 11, 12, 13), suggesting when the public has a better understanding of the value of research, they are more supportive of the use of their data for that purpose.

These findings demonstrate the need for transparency and effective communication of the use of administrative data for research and its benefits. These communications should be accessible to a wide public audience in terms of both the language and platforms used, and focus on what appears to be the most essential condition of research using administrative data: public interest.

5 Public interest

The literature has found public interest (or ‘public good’, ‘public benefit’, ‘social value’) to be the primary driver of support for administrative data research (8, 9, 14, 15).

A public consultation by Ipsos MORI (16) on behalf of the Medical Research Council regarding the use of personal health information in research found 70% of participants agreed the advantages of medical research outweigh the disadvantages. Of respondents to the 2015 Northern Ireland Life and Times (NILT) Survey (17), 85% agreed: ‘if personal data can be made anonymous and a person’s right to privacy maintained, then the data should be used where there is a benefit to society’ (p.22).

The public have been found to consider financial profit an unacceptable motive for the use of data (18, 19). A 2014 study by Marion Oswald investigating attitudes towards sharing personal data with the public sector (20) found most participants would be comfortable with their data being used to improve public services, but only around a quarter were comfortable with it being used to make profits to fund public services. Previous research has also identified concerns that some research using administrative data could inadvertently work against the public interest, for instance by causing demographic groups or local populations to be profiled (8, 9). Study participants have also expressed concerns that policy based on analysis of large datasets may not account for individual needs (8).

Previous literature has, however, found no widely understood definition of ‘public interest’ amongst the public, and perhaps what matters more than defining the term is that the public perceives benefits of some sort. Understanding what the specific communities the research aims to impact perceive as the benefits of the work therefore remains an important goal of public engagement.

5.1 Data types

The literature reviewed has identified differences in the perceived sensitivity of, and potential benefit of, using different types of data for research. During the ‘Dialogue on Data’ (9), some participants expressed that some data types — for example, records relating to domestic violence and HIV status — were too sensitive and personal to be shared outside of the agency that collected it. Nevertheless, by the end of the Dialogue the researchers found: ‘once there are strong researcher approval and security processes in place, [participants] were happy for data linking to go ahead using all types of administrative data’ (9, p.40.).

A 2018 discrete choice experiment by Aitken et al. (14) found the type of data being linked to be the most influential factor shaping preferences towards the linking of health data for research. How profits are managed and shared was found to be the second most influential factor, with the purpose of the research coming third. Meanwhile, 2013 research by the Wellcome Trust (21) found many regarded personal health data differently to other types of data. This rested upon a perceived ‘unquestionable benefit to people’ of experts having access to this type of information, especially in relation to illness (21, p.11).

5.2 Demographic differences

Previous literature has also found demographic differences in levels of public support for administrative data research. Younger age groups have in some instances been found to be more supportive of data sharing for research than older age groups (14, 21), though Stockdale et al.’s literature review (15) found evidence of both younger and older age groups being in favour of data sharing.

Aitken et al. (14) found participants not in full-time employment were more concerned with ‘oversight arrangements’ — or regulation measures — and the type of data being linked than those in full-time employment. Those working full-time were more concerned with the purpose linking, who the researchers were and profit management. The Wellcome Trust (21) reported
participants from socio-economic group C2DE (those in skilled, semi-skilled and unskilled manual jobs or on low or no income) felt more powerless to deal with the consequences of a data breach than those from socio-economic group ABC1 (managerial, administrative and professional, and supervisory and clerical jobs). Participants from group ABC1 were found to be more likely to view health data research as socially beneficial. These demographic differences suggest some areas of research may be more acceptable than others to the specific demographic groups whose lives they aim to benefit. It is therefore important to involve the publics most relevant to specific areas of research in engagement activities, so the views of the communities most affected by the work are sufficiently understood.

6 Privacy and security

Safeguards to protect the privacy of data subjects and prevent data from being misused have also been identified as key to public support for the sharing and use of administrative data. The main concerns identified can be broken down into de-identification and anonymisation; data access and security; and governance and regulation.

6.1 De-identification and anonymisation

De-identification or anonymisation appears to be the absolute minimum standard expected for the use of administrative data in research to be acceptable. Across the literature reviewed, study participants were found to be significantly more comfortable with their data being collected, stored and used when anonymised (8, 9, 10, 19, 20, 22). Most participants of the ‘Dialogue on Data’ (9) no longer considered de-identified data as ‘personal’ and had no concerns around the use of such data.

For the 85% of respondents of the 2015 NILT Survey who agreed data should be used where there is a benefit to society, this was based on an assurance that data would be anonymised (17). Ipsos MORI’s consultation (16) found 62% of respondents would be ‘certain or more likely’ to provide their health information if there were assurances of confidentiality (p.9). Participants of Wellcome’s attitudinal work (21) had a strong sense of personal health data as ‘confidential, private and sensitive’, and not to be shared outside of ‘secure, authorised bodies such as the NHS’ (p.3). Population-level data, however, was regarded as anonymous, and to be collected for the common good.

Participants of some studies, however, raised concerns re-identification of individuals if linked data, for example, included information that was unusual and might only apply to a small number of people (9, 12, 13, 15). Nevertheless, for most of the studies reviewed, respondents were largely supportive of data sharing when de-identification or anonymisation was guaranteed.

6.2 Data access and security

Study participants have expressed concern about data being leaked, lost, stolen or subject to unauthorised access and used against the public interest – whether de-identified or not – with additional safeguards to protect data therefore being considered critical (9, 15, 16, 21, 22).

Participants of the ‘Dialogue on Data’ (9) were in favour of secure physical settings and concerned about remote access to a secure environment. However, the authors found ‘the key idea that the data doesn’t leave the physical setting even when the researcher is working on it from a remote setting didn’t make intuitive sense to most’, and stress further work on how best to explain the concept is needed (9, p.46). Those who generally thought de-identified data is very low risk were more comfortable with remote access if protections were in place. Participants of the Dialogue also felt reassured there were no plans for a so-called ‘super database’ under ADRN, containing multiple linked datasets. However, this appears to have been a spontaneous consideration of participants, and the authors do not explain what such a database was understood to be.

Stockdale et al. (15) found participants were concerned that sharing their electronic health records (EHRs) may lead to them being leaked or used to their disadvantage, whilst Wellcome (21) found the same for the sharing of personal data more generally. Participants of Davidson et al.’s 2012 and 2013 consultations exploring attitudes towards cross-sectoral data sharing echoed this, with participants of the 2012 study (12, p.iv) fearing data linking would increase the likelihood of security breaches as hackers could obtain a large amount of information “in one hit”.

6.3 Governance and regulation

In addition to the physical security of data and controls around access, previous literature has identified a preference for protections in the form of governance and ethical frameworks to regulate data use.

In their reviews of previous literature, both Aitken et al. (8) and Stockdale et al. (15) identified an increase in public acceptance after study participants were informed of governance mechanisms. Davidson et al. (12) identified concerns about who would oversee data sharing frameworks and where accountability would lie if linked data were lost. Ipsos MORI (16) and Davidson et al. (19) both identified preference for an independent organisation.
to act as a ‘buffer’ between researchers and the public (16, p.7). In Aitken et al.’s exploration of attitudes towards the use of health data (11), however, participants expressed concern that committees of oversight bodies would by default operate in favour of data sharing.

Ultimately, for data use to be publicly acceptable, a myriad of safeguards are needed to protect the confidentiality of data subjects and limit the potential for misuse.

7 Trust and transparency

Previous literature suggests those sharing and using data must be trusted to keep it secure and be motivated by the public interest. Meanwhile, it also indicates that the specifics of projects using data affect public support, and transparency is key to allowing the public to remain informed about how their data is used in any given context.

7.1 Trust

The literature reviewed found clear differences in the levels of trust attributed to different types of organisation, with the reasons given providing indications as to how an institution or individual might be able to build trust.

Commercial organisations have been found to receive lower levels of trust than public bodies. Work by NatCen exploring Health Survey for England (HSE) participants’ attitudes to data linkage (13) found government collecting data in the form of the Census, and health data collected by the NHS, was considered important for future planning. However, it was felt commercial companies would only want to access data for commercial gain.

Participants of Davidson et al.’s workshops (19) expressed that who was accessing data and for what purpose is of greater concern than the type of data being accessed. They demonstrated ‘near universal acceptance’ of public bodies accessing anonymised data from other public sector organisations for research, driven by a perception that these organisations are dedicated to delivering public benefits and safeguarding data (19, p.8).

Participants of the ‘Dialogue on Data’ (9), however, were worried about access to government data by commercial companies due to low trust in government. For those who were more trusting of government, its use of data was seen as in the public interest. The Wellcome Trust’s attitudinal work (21) identified some cynicism, driven by fears about government ‘taking something away from people’ (p.9).

Furthermore, not all public bodies receive the same levels of trust, with previous literature identifying greater public trust in the NHS – particularly GPs – to keep information secure than in other types of public body (16, 17, 20, 22). Davidson et al. (12) found trust in the NHS to rest upon a perception that health professionals serve to help the public and abide by a moral code of conduct, supposedly more so than other public bodies.

Some study participants have also identified public benefits of private companies having access to data in certain circumstances. In such cases, there has been a preference for greater safeguards and controls than might be expected for public bodies (11, 18). Aitken et al. (11) found that, although some organisations are trusted more than others, this does not mean access to data by these groups is automatically supported, and vice versa.

Participants of the “Dialogue on Data” (9) felt researchers who gain access to linked data should be ‘unbiased’ and ‘qualified’, whilst researchers working for private companies should not have access (p.43). Participants of Aitken et al.’s discrete choice experiment (14) felt most comfortable with university or government researchers and NHS staff accessing data, while Aitken et al.’s focus groups (11) revealed a feeling that academics were less likely to be motivated by profit than other researchers.

These findings suggest that, to develop and maintain trust, an individual or organisation must demonstrate dedication to the public interest and safeguarding data. However, the findings also show trust is not straightforward; in some cases, lower trust may simply mean a need for greater data protections and stronger assurances of public interest.

7.2 Transparency

Participants of the studies reviewed expressed a desire for greater transparency in general around how administrative data is held and used, with efficient communications around data use being seen to have a direct impact upon public acceptability (8, 10, 13, 15, 16, 22).

Participants of the ‘Dialogue on Data’ (9) expressed concern the general public would not understand the process and purpose of administrative data research. Nevertheless, it was seen as important to communicate that data is anonymised; safeguards are in place; research is socially beneficial; and, in the context of ADRN, it would make existing data sharing frameworks more efficient.

Participants of citizens’ juries conducted by Tully et al. investigating public attitudes towards uses of health data (18) felt the public benefit of data use by commercial organisations must be made explicit. Aitken et al.’s focus groups (11) found concerns about data linking stemmed directly from a perceived lack of openness about data use, with participants saying it may be a deliberate effort to ‘withhold information’ (p.718-719). They also found transparency to play an important role in trust. Participants of NatCen’s study (13) who previously disagreed to have their HSE data linked to other forms of data recalled the main reason being a lack of information about how it might be linked.
These findings suggest transparency has a direct impact on public support for data sharing initiatives. Without the relevant information being publicly available, an initiative may experience a lack of support, and if those handling and using data are transparent about how and why it is used, they are likely to receive a greater level of trust.

8 Striking the balance

No study has identified any sole assurance that is enough to secure public support for research using administrative data. Rather, all have highlighted that support cannot be guaranteed without fulfillment of all three core conditions: public interest, privacy and security, and trust and transparency.

In the ‘Dialogue on Data’ (9), alongside tangible ‘social value’, ‘data is de-identified’, ‘data is kept secure’ and ‘businesses are not able to access the data for profit’ were also considered necessary for public support (p.7). The 2015 NILT Survey (17) found support for data sharing to rest upon ‘three pillars’: trust in organisations, data protection measures and public benefit (p.25). If any are reduced or removed, public support falls. Stockdale et al.’s review of previous literature (15) found while there was a general willingness to share patient data for research, ‘this very rarely led to unqualified support’ and rested upon data security and the motivations for using the data (p.1).

However, public support is not straightforward, and the literature shows the specifics of any given project have an impact on public expectations of the required standard of each core condition. Participants of previous studies have expressed that they do not expect even the highest level of data protection to be entirely ‘foolproof’, but the public is comfortable if this is outweighed by the potential benefits in each case (8, 9, 10). There is an understanding that there is always some level of risk to privacy and potential for misuse associated with the use of data.

Work by the Royal Statistical Society (RSS) exploring public attitudes towards data linking and privacy (22) found 35% of respondents disagreed that, once their data has been anonymised, ‘I’m not really bothered how it is used’, showing a notable proportion continued to care about the specifics of data use (p.3). Work by the UK Office for National Statistics (ONS) (10) similarly found public views towards the use of data for research to differ according to who is using the data and what for.

Ipsos MORI (16) identified a tension between the ‘greater good’ and individual privacy (p.7). 69% of participants were ‘likely’ to allow personal health data to be used for research – suggesting the specifics of the research are important – compared to only 14% who were ‘certain’ to (16, p.8). Oswald et al. (20) found that the ‘benefits-versus-costs problem’ is significant; the more tangible the benefit, the greater the comfort in data sharing (pp.270-271).

These findings show public support for research using administrative data is complex, and some projects may require the assurance of greater safeguards than others if aspects of their approach are considered less robust, even once a certain standard of each of the necessary conditions is achieved. In conclusion, the potential public benefits must ultimately outweigh the risks to privacy and the possibility of misuse, and an appropriate balance of all three core conditions must be struck to achieve this.

9 Beyond transparency

In addition to exploring the attitudes and sentiments of the public towards administrative data research, previous literature has given important indications as to the type of engagement and involvement the public expect to have.

Emily Rempela et al. (23), concluding a literature review of public engagement in new technologies, stress transparency is not enough and argue data science initiatives should involve the public in technological development. This participatory approach, the authors say, is more effective at having an impact than one-way communications. They stress that while widespread consultations such as the ‘Dialogue on Data’ represent a step towards understanding public views, they ‘do not equate nor reflect public influence’ (23, p.575).

Aitken et al.’s focus groups (11) found preference for an ‘open exchange of information and greater equity in the science-public relationship’, in which public engagement is an indicator of the trustworthiness of data users rather than a way to build trust (p.719). The authors stress transparency must involve ‘open communication of uncensored information’, with trustworthiness more likely to be achieved if engagement involves open dialogue in which public concerns can be responded to (11, p.719).

These findings largely suggest public engagement should move beyond transparency and past widespread, general consultation on the use of data for research. It should now build upon existing knowledge about public attitudes as set out in previous literature and focus on gaining public input in specific areas of research.

10 Conclusion

This review shows the UK public are broadly in favour of administrative data research if three core conditions are met: public interest, privacy and security, and trust and transparency. Ultimately, the proposed benefit must outweigh the potential risk, and this is dependent upon the specifics of a project, including: the data being used; the questions being investigated; the protections in place; and who is accessing the data. These attitudes have been held
over time, with this review covering studies conducted between 2006-2018. Nevertheless, it is important to note that the nature of research is such that it is not always possible to know if it will ultimately prove beneficial. The findings are not known at the start, and all that can be aimed for is intended benefit.

Most previous consultation has focused on capturing the general attitudes of the public towards the sharing, linking and use of data in general on a broad scale. However – with the exception of medical research – there has been little that has focused on capturing the interests and concerns of the demographics and communities whose data is to be used for specific areas of research, whether this be in relation to crime and justice; inequality and social inclusion; or any other subject area. A thorough understanding of the interests and concerns of those with lived experience of an issue would be extremely valuable to ensuring research has the greatest impact possible.

In light of the findings of this review and due to the volume of existing literature on general attitudes towards the use of administrative data more broadly, and the consistent findings it has had, it is appropriate to move beyond widespread, general consultation about whether administrative data should be used for research. It is now important to focus on the specific issues being investigated using administrative data by seeking the input of specific demographics and communities in the research programmes that affect them. Nevertheless, it is important to continue to monitor any changes to broader public attitudes and adapt approaches if necessary.

Acknowledgements

ADR UK is funded by the Economic & Social Research Council (ESRC), part of UK Research & Innovation (UKRI), for an initial three years from July 2018 to July 2021, with the Strategic Hub funded until March 2022.

References

1. Digital Economy Act 2017. Disclosure of information for research purposes. Digital Economy Act 2017 part 5: Chapter 5, Section 64 (accessed 27/04/2020).
2. Information Commissioner’s Office. Anonymisation: Managing data protection risk code of practice. 2012.
3. Stokes P. The ‘Five Safes’ – Data Privacy at ONS. Office for National Statistics. 2017 Jan [accessed 17/04/20/]
4. Digital Economy Act 2017. Research Codes of Practice and Accreditation Criteria. Digital Economy Act 2017 part 5: Codes of Practice. Updated 2020 Feb (accessed 27/04/20/)
5. Information Commissioner’s Office. What is personal data? Guide to the General Data Protection Regulation (GDPR) (accessed 31/07/20).
6. Rowe G, Frewer LJ. A typology of public engagement mechanisms. Science, Technology & Human Values. 2005 April;30(2):251-290. DOI: 10.1177/0162243904271724.
7. Information Commissioner’s Office. Principle (a): Lawfulness, fairness and transparency. Guide to the General Data Protection Regulation (GDPR) (accessed 17/04/20).
8. Aitken M, de St. Jorre P, Pagliari C, Jepson R, Cunningham-Burley S. Public responses to the sharing and linkage of health data for research purposes: a systematic review and synthesis of qualitative studies. BMC Medical Ethics. 2016;17(73). DOI: 10.1186/s12910-016-0153-x.
9. Cameron D, Pope S, Clemence M. Dialogue on Data: Exploring the public’s views on using administrative data for research purposes. Ipsos MORI Social Research Institute. 2014.
10. Office for National Statistics, The Census and Future Provision of Population Statistics in England and Wales: Public attitudes to the use of personal data for official statistics. 2014 March.
11. Aitken M, Cunningham-Burley S, Pagliari C. Moving from trust to trustworthiness: Experiences of public engagement in the Scottish Health Informatics Programme. Science and Public Policy. 2016 May 11;43(5):711-723. DOI: 10.1093/scipol/scv075.
12. Davidson S, McLean C, Cunningham-Burley S, Pagliari C. Public acceptability of cross sectional data linkage: Deliberative research findings. Scottish Government Social Research. 2012 Aug.
13. Davies M, Jones H, Conolly A. Public Attitudes to Data Linkage: A report prepared for University College London by NatCen Social Research. NatCen Social Research. 2018 March.
14. Aitken M, McAtee G, Davidson S, Frostick C, Cunningham-Burley S. Public Preferences regarding Data Linkage for Health Research: A Discrete Choice Experiment. International Journal of Population Data Science. 2018;3(11). https://doi.org/10.23889/ijpds.v3i1.429.
15. Stockdale J, Cassell J, Ford E. “Giving something back”: A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland (Revised). Welcome Open Research. 2019 Jan;3(6). https://doi.org/10.12688/wellcomeopenres.13531.2.
16. Ipsos MORI. The Use of Personal Health Information in Medical Research: General Public Consultation. Medical Research Council. 2007.
17. Robinson G, Dolk H, Dowds L, Given J, Kane F, Nelson E. Public Attitudes to Data Sharing in Northern Ireland: Findings from the Northern Ireland Life and Times Survey 2015. Ulster University. 2018 Feb.
18. Tully MP, Hassan T, Oswald M, Ainsworth J. Commercial use of health data – A public “trial” by citizens’ jury. Wiley: Learning Health Systems. 2019;3. https://doi.org/10.1002/lrh2.10200.
19. Davidson S, McLean C, Treanor S, Aitken M, Cunningham-Burley S, Laurie G, Sethi N, Pagliari C. Public acceptability of data sharing between the public, private and third sectors for research purposes. Scottish Government Social Research. 2013 Oct.
20. Oswald M. Share and share alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory research project investigating attitudes to sharing personal data with the public sector. SCRIPTed. 2014 Dec;11(3):245-272. DOI: 10.2966/scrip.110314.245.
21. Wellcome Trust. Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. London: Wellcome Trust. 2013 July.
22. Royal Statistical Society. Royal Statistical Society research on trust in data and attitudes toward data use/data sharing. 2014.
23. Rempela ES, Barnett J, Durrant H. Public engagement with UK government data science: Propositions from a literature review of public engagement on new technologies. Government Information Quarterly. 2018 Oct;35(4):569-578. https://doi.org/10.1016/j.giq.2018.08.002.