



Understanding
Patient Data



CarnegieUK
TRUST

CHANGING MINDS • CHANGING LIVES



Data for Public Benefit

Balancing the risks and benefits of data sharing

ABOUT THE PARTNERS:

Involve is the UK's leading public participation charity. We believe that people should be at the heart of decision-making. Involve gives people the power to take and influence the decisions that affect their lives; helps decision-makers to harness the potential of public participation; and supports people and decision-makers to collaborate to achieve social change.

Previously, Involve co-ordinated a two-year open policymaking process for the Cabinet Office to try to make progress in data sharing in three areas of proposed government legislation. The Digital Economy Act contains the provisions to turn these proposals into law. An important strand of the discussions during this process was around how best to define public benefit and balance it against privacy and wider risks. While significant progress was made, the discussion involved a small number of civil society organisations and focused around three relatively narrow areas of public policy. In addition, we believe that although the Act provides for some data sharing between government departments, it will not resolve the complex set of trade-offs between public benefit, privacy and security by itself.

The Carnegie UK Trust's Digital Futures theme seeks to maximise the ability for new technologies to improve wellbeing and mitigate the risks of the digital world for citizens. As part of this the Trust wanted to explore the trade offs we make between our personal privacy and giving others access to our data in order to provide us with goods and services.

The Carnegie UK Trust works to improve the lives of people throughout the UK and Ireland, by changing minds through influencing policy, and by changing lives through innovative practice and partnership work. The Carnegie UK Trust was established by Scots-American philanthropist Andrew Carnegie in 1913.

Understanding Patient Data supports better conversations about the uses of health information. Our aim is to explain how and why data can be used for care and research, what's allowed and what's not, and how personal information is kept safe. We work with patients, charities and healthcare professionals to champion responsible uses of data.

Lead Author: Kaela Scott.

Contributors: Simon Burall, Nicola Perrin, Philippa Shelton, Douglas White, Gail Irvine and Anna Grant.

April 2018



Contents

Foreword	2
Data for Public Benefit Summary	4
Executive Summary	6
1. Introduction	12
2. Data Sharing and Public Service Delivery	14
Drivers for greater data sharing	14
Understanding data sharing	14
A focus on personal data	15
Data sharing and privacy	15
3. Understanding ‘Public Benefit’ in the context of data sharing	17
Identifying the benefits of data sharing	17
Evaluating the relative value of different benefits	22
Conclusions following the workshop process	25
4. Identifying Dimensions of Risk	26
Conclusions following the workshop process	31
5. Determining acceptable uses of data to deliver Public Benefits	32
Principles for assessing public benefit	32
Conclusions following the workshop process	38
6. Moving Forward.... balancing the risks of using data against ambitions to deliver ‘Public Benefit’	39
Framework for Evaluating Public Benefit	39
Framework for assessing the merit of a data sharing activity to deliver ‘public benefit’	40
How this framework can be used within (and across) organisations	43
Involving the public in the discussion	43
Annexes	45
Annex A: Workshop Methodology	45
Annex B: Spectrum of Identifiability	47
Annex C: Legal Context for Data Capture and Sharing	48
Annex D: Defining Personal Data	50
Annex E: The Right to Privacy	51

Foreword

Involve, Understanding Patient Data and the Carnegie UK Trust all share a collective interest in how local and national governments, civil society and the public can have more effective conversations around data sharing, to enable better informed, consistent and transparent data decisions to ultimately create improvements in wellbeing for citizens.

Data – how it's acquired, stored, and used – is one of the great social, economic and cultural issues of our age. It has never been a more in-demand commodity. The ever-growing volume of data that we generate about ourselves, and which is generated about us, has profound effects on how we consume, work and live. The deployment of this data has produced a great many benefits, in particular the availability of content, goods and services which are unprecedented in their level of personalisation, speed and responsiveness. At the same time, the proliferation of vast amounts of data about who we are and how we live our lives brings significant risk, to our privacy, our autonomy and our sense of identity. Addressing these challenges and identifying where the acceptable trade-offs lie, appears certain to be a complex, high profile public policy priority for many years to come.

For public services, the collection, use and sharing of data is implicitly understood as vital to the provision of almost any effective service. However, despite the quantity of data that many individual public service departments hold and have access to, the landscape to utilise this data to best effect across different services remains complex and fragmented. Attempts at both national and local level to better share personal data in order to improve public service delivery for citizens' benefit have been challenged on the grounds of data security and individual privacy concerns.

In this context, Involve, Understanding Patient Data and the Carnegie UK Trust, organised workshops in six local authority areas to examine how the risks and public benefits associated with data sharing are recognised, quantified and evaluated by stakeholders. Ultimately we wanted to understand the data trade-offs that are currently being made every day across local government and civil society, and the reasons for these decisions.

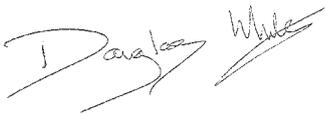
We found through our workshops a great deal of variation across services and localities in how public benefit and risk in data sharing are defined and balanced. We also found a real commitment and desire amongst public service providers to reach the best possible arrangements in each instance for citizens and communities, as well as a real appetite to engage in the debate in order to shape future change and improvement.

The purpose of our work was not to determine the absolutes of what is and what is not acceptable in terms of data sharing risks and benefits. Indeed, the workshops demonstrated just how difficult it is to reach a single common view. Our report is therefore designed to provide a framework to support government and civil society organisations at both national and local level, to define, assess and evaluate the public benefits that use of data may be able to deliver. This in turn will enable these organisations to more effectively, consistently and transparently balance the full opportunities that data sharing presents against the risks that it may incur.

In order for public service providers to be truly confident in data sharing decisions, it is vital that they are able to engage the public in an informed and meaningful dialogue, and to give communities the opportunity to shape the processes and systems through which decisions are made. We hope that our report can also provide a platform for the advancement of these conversations.

We are hugely grateful to all of our partners who supported us in this project. The input of Open Rights Group, the Office of the National Data Guardian and The Centre of Excellence for Information Sharing was critical in framing the project and supporting the workshop process. Our local partners Greater Manchester Connect, Sheffield City Council, West Midlands Combined Authority, Melton Borough Council, Essex County Council, Leeds City Council and Data Mill North generously hosted workshops and engaged public service providers from across a range of services in their area. We are thankful to them all.

We look forward to working with a wide range of stakeholders, at national and local level, from across the public service landscape, to help advance the issues and ideas set out in this report.



Douglas White
Head of Advocacy
Carnegie UK Trust



Simon Burall
Senior Associate
Involve



Nicola Perrin
Head of Understanding Patient Data
Understanding Patient Data

Data for Public Benefit Summary

POTENTIAL BENEFITS FROM DATA SHARING



Individuals

- Safeguarding
- Ensuring continuity of care and support
- Enabling the right services to be offered to individuals at the right time
- Co-ordinate of interventions and providing an integrated support service
- Connecting the administrative information held about citizens across departments to simplify and streamline consumer interactions
- Identification of people who might benefit from a new, or different, service offer
- Automatically provide citizens with benefits they are entitled to



Service Providers (Short-term)

- Reducing duplication and waste
- Supporting effective, better targeted front-line service delivery
- Directing resource allocation
- Identifying instances of fraud and/or debt
- Monitoring demand and delivery patterns
- Improving levels of customer satisfaction



Service Providers (Longer term)

- Producing local statistics
- Enabling the better monitoring and evaluation of service impacts
- Facilitating evidence based policy and decision making
- Identifying the root causes of problems
- Tracking a service user's journey
- Predicting future service needs
- Testing strategic and service planning hypotheses
- Developing shared outcomes and indicators across service providers
- Increasing public trust in government



Communities

- Providing intrinsic benefits to society through access to better public services
- Delivering improved outcomes for communities
- Enabling Research

POTENTIAL RISKS FROM DATA SHARING



Individuals

- Incursions into privacy from the use of identifiable personal information
- Risks from insecure data management and storage
- Risks from unintended re-identification
- Exposure to unwanted attention / service offers
- Punitive impacts



Service Providers

- Legal risks associated with data loss or misuse
- Loss of public trust from using data without consent
- Reputational risks from using sensitive personal data
- Risks from sharing data with organisations outside the public sector
- Using data for purposes that are not publically acceptable
- Risks to service provision from the use of unreliable data



Communities

- Stigma and discrimination
- The potential for negative impacts on communities from the selective use of data
- Loss of services

The effective use of data needs to meet three conditions:



Purposeful

- provides **direct and tangible benefits to individuals**
- delivers **positive social outcomes**
- impacts on **multiple beneficiaries** aligns with **public expectations** and does not over-step the boundaries of reasonable expectation
- achieves **long-term impacts** by addressing the root-causes of problems (for individuals or wider social issues)
- addresses a **significant social problem**
- **minimises negative effects**



Proportionate

- actively **minimises the amount of data needing to be shared**
- considers **whether personally identifiable data is necessary** to achieve the goal
- has **clear parameters** in order to protect against 'mission creep' and the risk of data being used for purposes other than which it was provided or shared
- considers the **likelihood of risks being realised** and balances the severity of a potential negative impact against this
- considers the **sensitivity of the data** being used and whether sensitive personal data is needed



Responsible

- is a **'good' use of data** i.e. is a more efficient and effective way to add significant value to decision making or policy implementation than other approaches
- has effective measures in place to ensure that the **data can be used and shared securely**
- will **deliver the intended outcomes**
- was **justifiable**
- is **defensible**

Involving the Public

Underlying all of this work is the need for informed and meaningful conversations with the public.

Evaluating Public Benefit (Full Framework on Page 40)

5 key features that a data sharing initiative designed to deliver public benefits should be able to demonstrate:

1. Enables high quality service delivery which produces better outcomes for people, enhancing their wellbeing.
2. Delivers positive outcomes for the wider public, not just individuals.
3. Uses data in ways that respect the individual, not just in the method of sharing but also in principle.
4. Represents, and supports, the effective use of public resources (money, time, staff) to enables the delivery of what people need/want from public services.
5. Benefits that are tangible, recognised and valued by service providers and the wider public.

Executive Summary

Data is frequently touted as the new oil; value is to be extracted from it in order to deliver services that the public wants and unlock new applications that will make their lives easier. This is as true for personal data held by the public sector as it is commercial data extracted from consumers.

Yet despite the many claims made for the public benefit which can be derived from the use of such personal data – and attitudes research that shows the public is much more likely to view data sharing as acceptable if there's a public benefit – the term 'public benefit' is rarely, if ever, clearly defined. In a context of significant concern about the public acceptability of much of the data currently shared, this presents public service providers with challenges in deciding when they should share data and for what purposes.

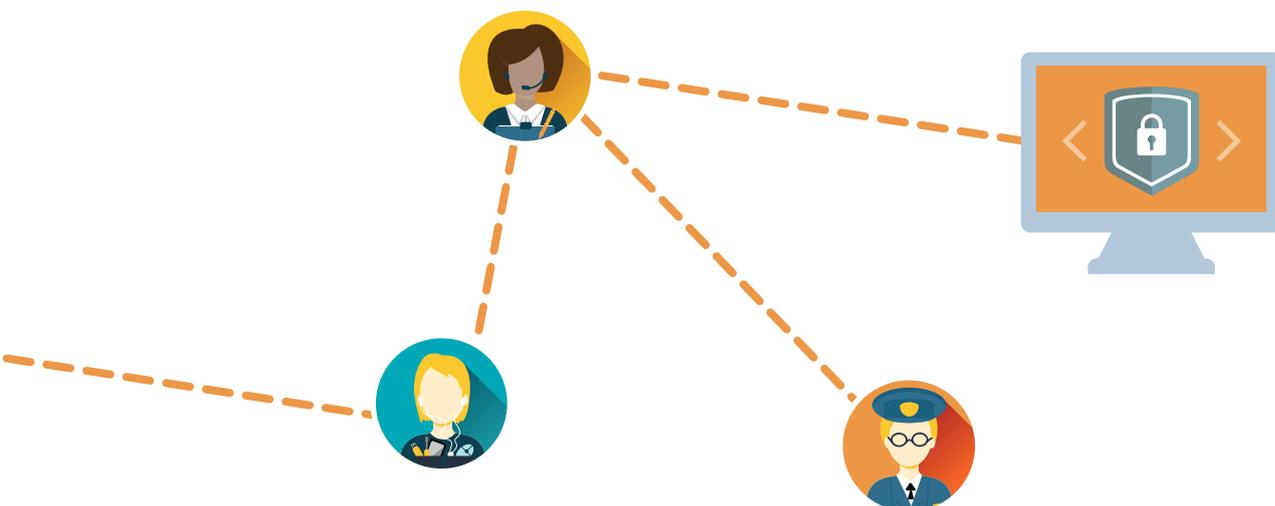
This report presents the findings from a series of six workshops in different local authority areas (Melton Borough Council, Essex County Council, Leeds and Sheffield City Councils, and Manchester and West Midlands Combined Authorities). These workshops brought together over 120 professionals from the public and voluntary sectors (working in the fields of housing, criminal justice, health, social care and welfare) to explore how they understand, define and value the public benefits which could be derived from the use of personal data.

This report establishes a framework for those providing public services to assess and evaluate the public benefits that the better use of data may be able to deliver and attempt to balance this against the risks sharing data may entail.

Determining acceptable uses of data to deliver Public Benefits

There are clear tensions between reaping particular benefits on one hand and mitigating the range of risks associated with sharing personal data on the other. Finding an acceptable settlement between these benefits and risks remains a key challenge for policymakers, frontline staff, advocacy groups and the public at large if the ambitions for data to be used as a tool for delivering public benefit are to be realised.

Three clear tests emerged throughout the workshops as being necessary for public service providers to gain the social licence to share and use data more widely.





a) Purposeful

When the purpose of a proposed use or sharing of data is clearly and transparently defined, participants were readier to accept a proposed use of data. It was also felt this helped provide protection (for both the data subject and the organisations involved) against data being used for purposes beyond that for which it was initially shared.

A number of additional factors impacted on assessments of purposes geared towards delivering public benefit, and the level of risk tolerable to achieve them, including that the use of data:

- provides **direct and tangible benefits to individuals**;
- delivers **positive social outcomes** (eg reducing social isolation, reducing inequalities or supporting local area regeneration);
- impacts on **multiple beneficiaries** eg on individuals, services and the wider public;
- aligns with **public expectations** and does not overstep the boundaries of what the public could reasonably expect data they had provided to be used for;
- achieves **long-term impacts** by addressing the root-causes of problems (for individuals or wider social issues);
- addresses a **significant social problem** ie when the initiative tackled important and complex social problems that other methods had failed to resolve;
- **minimises negative effects** (intended or unintended) for individuals and groups eg through excessive incursions into privacy; punitive action; stigmatisation/discrimination; or the diversion of resources from one area/sector of the population.



b) Proportionate

A number of factors contributed to assessments of proportionality in the workshops, including that the proposed use of data:

- actively **minimises the amount of data needing to be shared**;
- considers **whether personally identifiable data is necessary** to achieve the goal;
- has **clear parameters** in order to protect against ‘mission creep’ and the risk of data being used for purposes other than which it was provided or shared;
- considers the **likelihood of risks being realised** and balances the severity of a potential negative impact against this ie that the existence of even a significant risk should not automatically discount an opportunity being pursued;
- considers the **sensitivity of the data** being used and whether sensitive personal data is needed.



c) Responsible

Participants explored the idea that to be a justifiable use of public resources, the benefits likely to be achieved by a particular use of data have to be balanced not just against the risks, but against delivering the intended outcome.

A variety of factors were identified as contributing to whether a particular opportunity for data sharing could be considered an efficacious use of public resources, including that a proposed use of data:

- is a **‘good’ use of data** ie is a more efficient and effective way to add significant value to decision making or policy implementation than other approaches;
- has effective measures in place to ensure that the **data can be used and shared securely**;
- will **deliver the intended outcomes**;
- was **justifiable** ie that service providers could demonstrate that they had considered the potential impacts, done what they could to mitigate negative consequences, and ultimately determined that the benefits outweighed the potential for harm;
- is **defensible** ie that a service provider would be able, and willing, to make a publically acceptable defence of their decision to use data in a particular way if challenged.

Understanding 'Public Benefit' in the context of data sharing

Participants across the workshops focused on three groups which could directly benefit from the better use of data:



Individuals. There was significant support for using data to provide benefits directly to individuals, including for the purposes of, for example: **safeguarding**; ensuring **continuity of care**; **enabling service offers** to individuals at the right time; **simplifying user interactions** with services; **automatically providing citizens with benefits** they are entitled to.

Participants identified a number of criteria for determining whether such data sharing delivers public benefits: the **number of people** able to benefit; the perceived **level of need** for example, having direct impact on vulnerable groups (eg the homeless) and/or address key social problems (eg social isolation); and/or having **long-term impacts** on individuals and the services available to people.



Public Service providers. There was a high level of support for using data to enable services to be delivered more efficiently and therefore to support them to 'do more with less', for example, by **reducing duplication and waste**, **supporting better targeted front-line service delivery** and/or **directing resource allocation**.

Participants also identified the benefits that a more open flow of data between service providers could bring for **developing joint work focussed on outcomes**, **evaluating service impacts**, **identifying the root causes of problems** and **predicting futures service needs**.



Communities. Effective use of data should be able to deliver wider, positive social outcomes beyond the benefits delivered to individuals and services. Dimensions of this type of benefit include: **providing intrinsic benefits to society through access to better public services**; **delivering improved outcomes for communities**; and **enabling research**, even if those benefits may be less tangible and not immediately apparent.

Overall, the discussions at the workshops clearly demonstrated that each decision to share personal data needs to be assessed on its own merits; there is no simple definition of public benefit which can be applied; and that, at present, approaches to identifying and classifying benefits are inconsistent. Despite lacking a common framework to follow, the three dimensions of public benefit are clear.



Identifying Dimensions of Risk

The majority of the debate and concern about risks from sharing personal data focuses on the privacy of the individual whose data is being shared. Throughout the workshops, however, participants raised a far wider range of risks to individuals, organisations and the wider community. This suggests that there is a need for a renewed and deeper societal debate to understand the extent to which the public share the same concerns and where the deepest public disquiet lies.

The risks identified at the workshops can be summarised as being to three groups:



Individuals. Risks relating to individual privacy ranged from concerns about **insecure data management and storage** and **unintended reidentification** to the wider concern that to deliver the types of benefits outlined above, would require **the use of types information that many people would consider private**, and may simply want to keep that way.

Participants were also concerned sharing personally identifiable information (particularly without the direct consent of the individual) could **expose individuals to unwanted or inappropriate offers of service**. Data sharing initiatives that resulted in **punitive impacts** for individuals also received a mixed response from participants, particularly when data obtained for a different purpose was used to deliver these consequences.



Communities. Concerns were raised that sharing and linking data for the purposes of targeting public services, even if the information used was not personally identifiable, could result in the production of generalisations that categorise individuals, social groups or geographic areas in ways that could result in **stigma, lead to discriminatory treatment, or inappropriate targeting**.

Participants were also concerned about poor data quality leading to false conclusions being drawn leading to, for example, evidence being developed for advocacy or targeting resources differently. Further, as data may be able to support agencies to more effectively allocate resources, it can also be used to **reduce or remove services from areas or communities**. While these decisions may be evidence based, they can still lead to feelings of loss among communities.



Public Service Providers. **Legal risks associated with data loss or misuse** are perennial concerns for service providers. However, even if a data use may be legally compliant, that may often not be enough to assess it as being of low risk; service providers also identified risks associated with **loss of public trust from using data without consent** (even if legally permitted) or for purposes **unacceptable to the public**, for example.



Developing a framework to balance risk and benefit

Choices about what data public service providers use and share, and for what purposes, requires them to balance and assess the relative benefits and risks to individuals, the wider public, and services themselves. While there are a variety of privacy impact assessment tools and planning frameworks that have been produced to assist organisations in assessing opportunities for data sharing within and between organisations most of these tend to focus on aspects of the data itself. To date however, very little focus has been given to supporting organisations to evaluate dimensions of benefit, assess the dimensions of risk and weigh up effectively the types of purposes that are valued most against the potential for harm.

Our analysis of the debates and deliberations that took place across the workshops has

identified points of common ground that, together, encapsulate the elements necessary for a data sharing initiative to be described as producing 'public benefit'.

The framework we have developed sets out a series of evaluative questions, grouped around each of these features, to help service providers and data controllers (in the first instance) clarify the potential public benefits of using and sharing data to deliver public services and consider the risks involved in doing so. The questions have been selected in order to initiate discussions about the various dimensions that data sharing proposals can be measured against and, while not exhaustive, our research suggests that collectively they provide an effective framework for assessing the acceptability and relative merit of data sharing initiatives intended to deliver 'public benefit'.

Evaluating Public Benefit (Full Framework on Page 40)

We conclude that there are five key features that a data sharing initiative designed to deliver public benefits should be able to demonstrate:

1. That it enables high-quality service delivery which produces better outcomes for people, enhancing their wellbeing;
2. That it delivers positive outcomes for the wider public, not just individuals;
3. That it uses data in ways that respect the individual, not just in the method of sharing but also in principle;
4. That it represents and supports the effective use of public resources (money, time, staff) to enables the delivery of what people need/want from public services;
5. That the benefits are tangible, recognised and valued by service providers and the wider public.

The framework we have developed presents each of these features alongside a set of evaluation questions that can be applied assess the potential of a data use to deliver public benefit.

Moving forward...

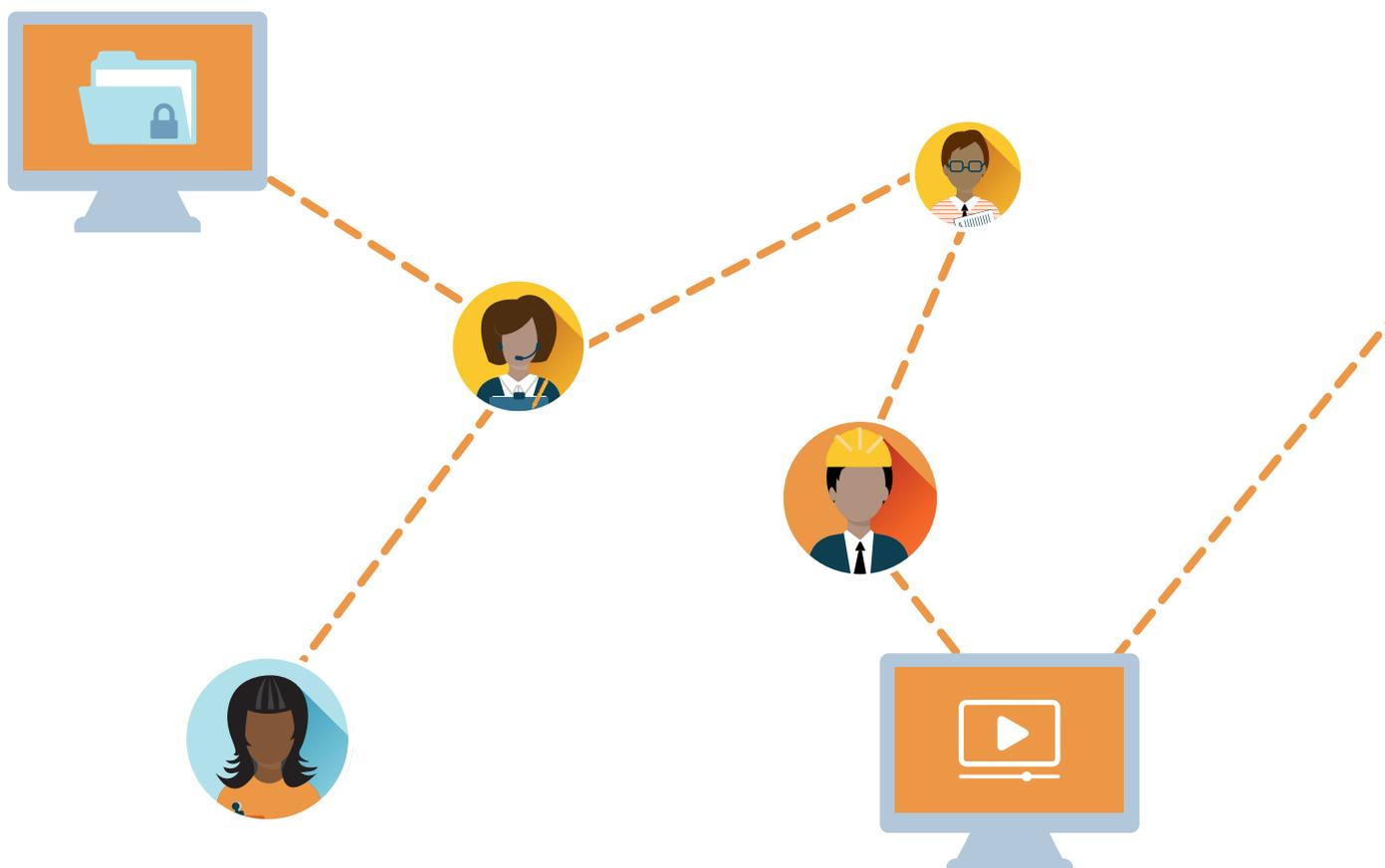
For organisations and partnerships that want to unlock the potential of the data they and other services hold about citizens, developing a shared understanding of the public benefits people want and expect from data use, and a consistent language with which to talk about them, is vital.

Working through the questions presented in this framework with staff, partners and other stakeholders will help service providers clarify their own understanding of the benefits and risks associated with the wider use of data and become better able to articulate, and/or justify, the decisions they may make. This, in turn, will help set the stage for a wider, national strategic discussion that could help nurture a more coherent approach to balancing the risks of using data against the goal of delivering 'public benefit'.

If the social licence for greater data sharing is to be realised the basis of delivering public benefit,

then the public also need to have the opportunity to be involved in the discussions. This needs to be undertaken in ways that enable the public to help shape the future of data use by engaging in informed and meaningful dialogue with service providers regarding their aspirations for how public services should be provided and their concerns about how data about them should be used. This framework will also provide a useful tool for initiating these conversations with service users, community representatives, and ultimately the wider public, in ways that will increase their understanding of the complexities involved.

While in the short term, the efforts required to begin this process are not insignificant, in the long term, the costs to service providers of not taking the public with them on this journey are likely to be much higher. To not begin these conversations now may undermine the reputation of public service agencies, hamper their ability to resolve disputes, and ultimately constrain their ability to use data in modern, beneficial and potentially transformative ways.



1. Introduction

Government and other agencies providing public services increasingly collect, store and use personal data about citizens as a standard part of the business of delivering services.

It is widely held that more effective use of this data could support agencies to provide better targeted, more efficient services in ways that deliver clear ‘public benefits’. This concept of ‘public benefit’, however, is rarely defined, and it can often mean very different things to different people in different contexts.

This prompts fundamental questions about what the public views as acceptable use of the data held about them by public service providers, and for what purposes these providers should have a social licence¹ to use and share this data in the pursuit of improved service delivery. Without a clear understanding of the public benefits that may be possible to achieve through the better use of data, and a shared language with which to discuss these benefits, these questions are difficult to answer.

In order to establish a better understanding of the issues at the heart of this impasse, Involve, the Carnegie UK Trust and Understanding Patient Data organised a series of workshops in diverse local authority areas across England during the summer of 2017. These workshops brought together professionals from the public and voluntary sectors to explore how they collectively understood, defined and valued the public benefits that may be delivered by the use of personal data about service users and the wider public. The purpose was to begin to make sense of where an acceptable balance may lie between the risks and benefits of data sharing and use in the context of public service provision.

This report is informed by the findings from these workshops, alongside information drawn from a

1 Social Licence is a term emerging from debates about data sharing that are taking place in New Zealand and rests on the assumption that ‘when people trust that their data will be used as they have agreed, and accept that enough value will be created, they are likely to be more comfortable with its use.’ Data Futures Partnership (2015) What is Social Licence? <http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/social-licence/> (accessed 2/6/2017)

review of relevant literature on public attitudes to data sharing. It establishes a proposed framework for service providers, across the public and voluntary sectors, to both evaluate the public benefits that the better use of data may support; and assess this potential benefit against the risks that sharing data may entail.

Overview of the workshops

The Better Use of Data: Balancing Privacy and Public Benefit workshops were designed to bring together a wide range of professionals working in the housing, criminal justice, health, social care and welfare sectors² to define and evaluate the ‘public benefits’ that may be delivered by the better use of data; consider the risks involved in data sharing; and begin to make sense of where an acceptable balance may lie between these risks and benefits.

In each area, the workshops were hosted by a local authority partner. These were:

- Greater Manchester Connect;
- Sheffield City Council;
- West Midlands Combined Authority;
- Melton Borough Council;
- Essex County Council;
- Leeds City Council / Data Mill North.

In the workshops, a series of examples and case studies were used to prompt discussions.³ These case studies illustrated how data is

2 While recognising that the issues and debates surrounding data sharing cut across all aspects of public service delivery, the decision to focus this project on these areas of public service delivery was based on clear evidence of increasing demand within these sectors for the sharing of personal data to support more effective multi-agency working at a local level. Further, in all of these fields, decisions about what data to share, when to share it, and who to share it with have potentially significant impacts for individuals and create challenging ethical dilemmas for professionals.

3 The examples prepared by Involve for use during the workshops can be viewed at <https://www.involve.org.uk/wp-content/uploads/2017/07/workshop-examples.pdf> and the case studies at <https://www.involve.org.uk/wp-content/uploads/2017/07/3-case-studies-data-sharing.pdf>

currently being shared and used by public service providers across the country for a variety of purposes. Building in complexity throughout each workshop, these case studies were used to challenge participants to develop shared criteria to assess the relative acceptability of using different types of data for different purposes.

Throughout the workshops, participants also benefited from expert input from [Understanding Patient Data's](#) research into the best language to use when discussing the different forms in which personal data can be shared⁴; members of the [National Data Guardian's Panel](#) highlighting how challenges in relation to data sharing are being navigated in a health and social care context; and the [Open Rights Group](#) discussing the risks and opportunities associated with data sharing. A more detailed description of the rationale for the workshops, an outline of the methodology used and an explanation of how participants were selected can be found in Annex A.

In total, over 120 participants took part in these workshops – from city, borough and county councils, the Police, the Fire Service, the NHS, Housing Associations, Universities and voluntary sector organisations working in health, care, consumer advocacy and welfare – each bringing their own perspectives, experiences, reservations and aspirations to the discussion.

At the conclusion of the workshops, a series of standalone area reports were prepared and distributed to workshop participants to support the continuation of the local dialogues that the process had initiated.⁵

⁴ Understanding Patient Data's recent work on the best language to use when discussing identifiability and anonymisation with a non-expert audience, based on extensive testing with healthcare workers and the public, was used to frame the discussion of these issues during the workshops. This language will also be used throughout this report when referring to differing levels of identifiability and a summary is included with this report as Annex B. Understanding Patient Data (2017) What are the best words to use when talking about data <https://understandingpatientdata.org.uk/what-are-best-words-use-when-talking-about-data>

⁵ The 6 area reports can be accessed at <https://www.involve.org.uk/2017/07/17/theres-benefits-talking-data-sharing/>

Structure of this report

This report is intended to present an overview of the findings from the workshops in order to build an over-arching picture of how service providers from across these sectors understand and evaluate the potential benefits and risks associated with data sharing. It also looks at the impact this has on assessments of acceptable uses of data in the pursuit of public benefit.

While the findings from the six local workshops have informed the content of this report, the focus here is on the common and over-arching considerations, concerns and questions that emerged throughout the discussions.

Chapter 2 outlines the context of this research and the drivers for increased data sharing in the context of public service provision. It provides an explanation of key concepts and terms relevant to the debate in order to establish a shared understanding of themes explored in the body of the report.

Chapter 3 examines how workshop participants understood and evaluated the public benefit associated with data sharing and compares how this relates to public views on these benefits as evidenced through previous research.

Chapter 4 explores the risks participants identified in relation to the use of data by public service providers.

Chapter 5 focuses on how participants across the workshops assessed the overall acceptability of potential data sharing initiatives, balancing the trade-offs between benefits and risks to determine appropriate uses of personal data within the context of public service provision.

The final chapter reflects on what the findings mean for ongoing discussions about data sharing, public benefit and privacy in the UK and propose a framework for how assessments of public benefit might be advanced.

2. Data Sharing and Public Service Delivery

This section of the report establishes the wider context in which the research took place by outlining the drivers for data sharing in the context of public service provision. It also provides an explanation of key terms and concepts, and as such may be of particular value to readers less familiar with the topic.

Drivers for greater data sharing

Increased data sharing across and between public service providers is a cornerstone of ambitions to modernise government and transform the way public services across the UK are delivered. The overarching rationale behind the drive to extend the way data is used in public service provision is that the better use of data has the potential to:



produce direct benefits to individual service users by allowing more personalised and targeted services to be provided;



create wider public benefit by increasing the efficiency and effectiveness of public services overall; and



deliver social outcomes that enhance the wellbeing of people and communities.



'The ability to make easy data-driven decisions is becoming vital to the way that we all live and work. This should be the way that government provides services.'⁶

Understanding data sharing

The process of data sharing is, fundamentally, the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation. In the context of this report, the

term data sharing is used to cover both systematic, routine forms of sharing ie where the same data sets are regularly shared between the same organisations for an established purpose, as well as exceptional, one-off processes of data sharing for different purposes. It also includes data linking, where identifiable information from two or more data sets, from two or more sources is matched together.

Advances in information technology, alongside the rise in the number and type of organisations involved in delivering public services, have led to significant increases in the amount of data being produced across governments and other agencies in recent years. Moves towards e-government have also resulted in the automatic capture of vast quantities of data by public authorities as part of their routine business, for example for the purposes of registration, financial and service transactions or record keeping. For the most part, however, data generated across government and public service providers, is held and used solely within the organisation or department that collected it. This creates a situation where there can be both duplication and, potentially, contradiction in the datasets agencies hold, and effective data management is an ongoing challenge.

These same developments in information management and communications technology have also given organisations the ability to link and process large amounts of additional data. This enables information about a specific individual or an event to be linked and used in ways that are not possible using any single set of records separately and, if used effectually, can provide insight into how services can deliver better outcomes. However, it is not always easy for government and service

⁶ Cabinet Office (2017) Government Transformation Strategy. UK Government <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020> (accessed 28/5/2017)

providers to gain access to data held by other public service providers, particularly in a timely manner.

The legal context for data sharing between public agencies is complex and continually evolving.⁷ Until recently the ability to share data has tended to involve bespoke, bilateral legal gateways established for a specific purpose. The 2017 Digital Economy Act⁸ aims to streamline these processes for a limited number of areas of public service delivery by creating a more permissive environment for data sharing across and between agencies to support the better use of the information to inform policy, planning and service delivery.

A focus on personal data

The range of data collected by public service providers which could be shared to support public service delivery covers a wide range of operational and administrative information, for example service level performance and budget records, user satisfaction levels, impact monitoring statistics (eg reductions in ASB reports or homelessness figures) etc. This study, however, explicitly focuses on the sharing of personal information about individuals.

Using the definition of personal data included in the Data Protection Act,⁹ it is clear that personal information held by governments and public services could take many forms: from directly identifiable fields like name, address, biometric information or national insurance number, through to information like ethnic background, health records, disability, criminal record, income or credit history which, although not able to identify an individual in isolation, could render them identifiable if it was part of a collection of data held by an agency, or linked with data held by another agency.

Personal data can be shared and used in a variety of different forms, both anonymised and personally identifiable. The technical language of identifiability is complex and many different words are used to describe the same thing in different contexts (for example pseudonymised, key-coded, de-identified for limited disclosure). Throughout this report, the terms presented in Understanding Patient Data's Spectrum of Identifiability – personally identifiable, de-personalised and anonymous – will be used to distinguish between different levels of identifiability inherent in data use.¹⁰

Data sharing and privacy

A recent study into public attitudes to data sharing found that one of the top reasons for the public opposing the increased use of the data held about them was that: 'People have a right to privacy' (32%).¹¹ Individual privacy is defined by Privacy International as the conditions that enable people 'to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information'.¹²

The main threats to privacy from data sharing can be summarised as:

- the risk of data loss (through accident or malice)
- statistical disclosure (the potential to identify an individual within a dataset by their unique or rare combination of characteristics)
- the potentially negative impacts of secondary usage of data (through the disclosure or linking of information about a person that they would prefer to have remained private in a given context).

7 Annex C provides a more detailed summary of the legal context for data capture and sharing, as provided to participants in advance of the workshops to help inform their discussions.

8 UK Government (2017) Digital Economy Act <http://www.legislation.gov.uk/ukpga/2017/30/part/5/enacted> (accessed 28/5/2017)

9 UK Government (1998) Data Protection Act <https://www.legislation.gov.uk/ukpga/1998/29/contents> (accessed 28/5/2017) Further information about how the Data Protection Act defines personal data, and sensitive personal data, can be found in Annex D.

10 Understanding Patient Data (2017) What are the best words to use when talking about data <https://understandingpatientdata.org.uk/what-are-best-words-use-when-talking-about-data> Further definitions of these terms can be found in Annex B.

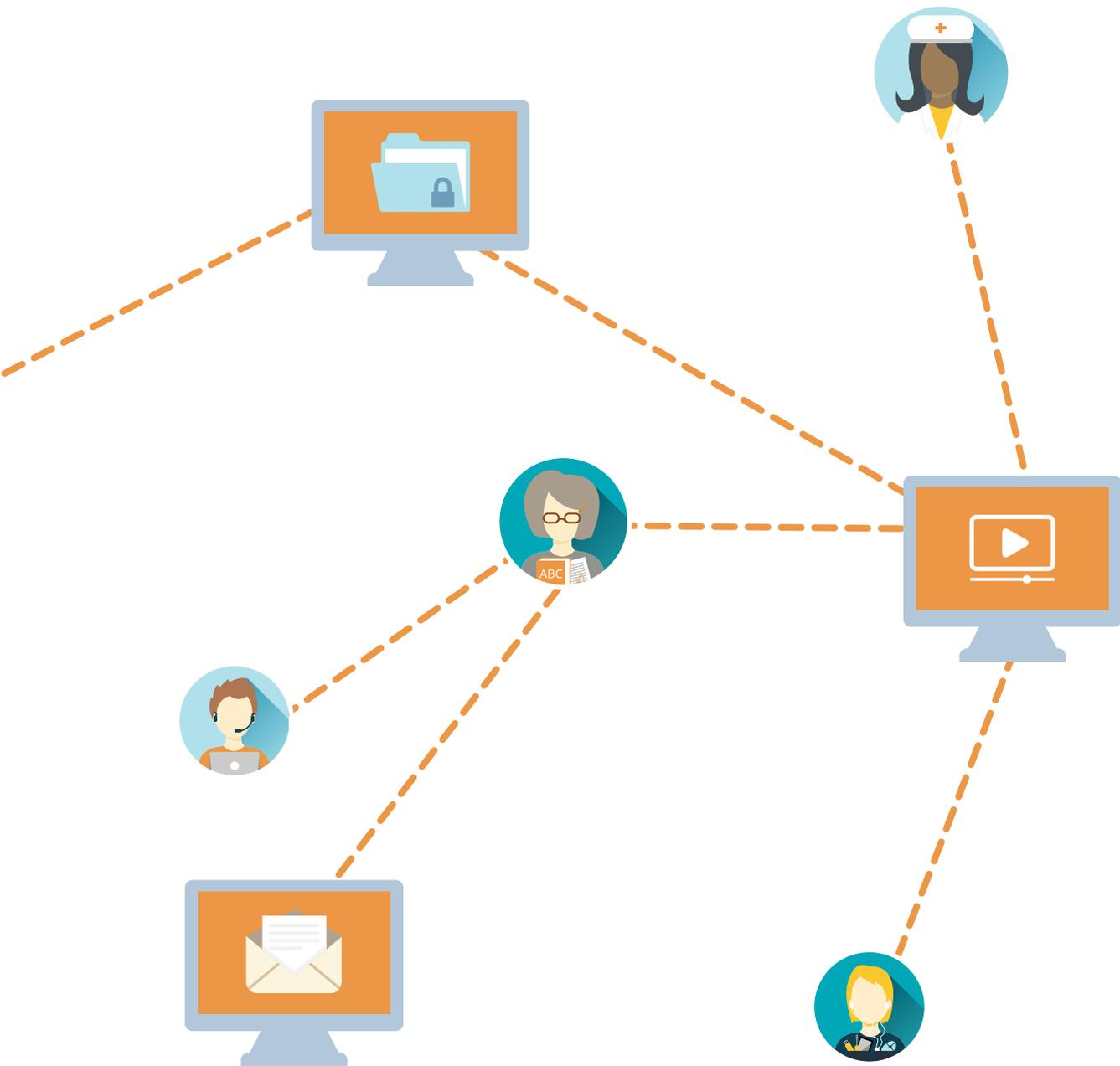
11 Ipsos Mori (2014) Public attitudes to the use and sharing of their data. Royal Statistical Society https://www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf

12 Privacy International (2017) What is Privacy? <https://www.privacyinternational.org/node/54> (accessed 28/5/2017)

The challenge of ensuring that data sharing practices within public service provision protect individuals' right to privacy, however, is not a new one. The UK is a signatory to the European Convention of Human Rights, so has incorporated the right to privacy into national laws. However, the

right to privacy is not an absolute right, and public authorities are permitted to share information without consent if there are lawful gateways and clear and proportionate reasons for sharing.¹³

¹³ More information about an individual's right to privacy can be found in Annex E.



3. Understanding ‘Public Benefit’ in the context of data sharing

The idea of delivering ‘public benefit’ is extensively used in policy documents and research reports to describe the purpose of data sharing. To date, however, there has been little examination of how either the public, or those involved in delivering public services, actually understand and evaluate the ‘public benefits’ that data sharing may be able to deliver.

The only formal definition of ‘public benefit’ that we were able to find during a review of literature undertaken for this project came from Statistics and Registration Services Act (s7(2)). It states that ‘public benefit includes in particular (a) informing the public about social and economic matters, and (b) assisting in the development and evaluation of public policy’.¹⁴ While this definition is functional, when interrogated in practice, it emerges as being both overly broad and, simultaneously, prescriptively limiting.

In order to move discussions forward about the potential benefits of data sharing, it is vital that proponents are able to clearly articulate the different dimensions of public benefit in ways that are easily understood and resonate with data controllers, service providers and the wider public. A key aim of this research was to develop a more nuanced understanding of how the concept of public benefit is understood by professionals involved in the delivery of public services.

‘If we can’t explain and demonstrate the benefits of sharing data, should we be doing it?’
WORKSHOP PARTICIPANT, ESSEX

Identifying the benefits of data sharing

Throughout all of the workshops, there was a general consensus among participants that service providers need data, and that there are many circumstances in which its collection and use to improve the delivery of public services is constructive and justified.¹⁵

Three groups of beneficiaries were focussed on by participants when identifying the different types of benefits that the better use of data could bring: individuals benefiting directly from the use of data collected about them; service providers deriving benefits from the use of personal data about service users or the wider public; and uses of data providing wider benefits for people and communities. The potential dimensions of benefits identified for each of these groups are outlined below.

a) Sharing data to provide direct benefits to the individual

There are a range of well-established practices for sharing personally identifiable data to support the provision of tailored and responsive services to individuals: between GPs and other branches of the NHS to ensure continuity of care; between social work services and the police to protect vulnerable adults; or between parole boards and housing authorities to ensure appropriate accommodation for offenders leaving custody.

14 UK Government (2007) Statistics and Registration Service Act <http://www.legislation.gov.uk/ukpga/2007/18/contents> (accessed 28/5/2017)

15 It does, however, have to be noted that the participants in the workshops were not recruited to be representative cross-section of practitioners in these fields. While every endeavour was made to ensure that in each area the group was as diverse as possible, the participants were invited from a self-selecting group who had expressed interest in spending a day exploring opportunities and challenges relating to increased data sharing in their local area.

Traditionally this type of information sharing has taken place directly between staff involved in providing services to the individual eg through discharge notes, case conferences or in response to a specific request. In each case, the ability to share information is permitted by legal gateways for data sharing and bespoke cross-sectoral agreements, which typically place constraints on information being shared on a 'need-to-know' basis and on what the information can be used for.

As we have already noted, the context of public service delivery is changing and becoming increasingly integrated: between government departments; through partnership work across the wider the public sector; and with commissioned agencies from the voluntary and private sectors. This is leading to new demands and expectations for data sharing in order to streamline the way services are delivered. The Digital Economy Act has responded to this by providing a new legal mechanism to enable greater data sharing between specified public-sector bodies and support the better use of data for defined purposes, including targeted interventions 'where its purpose is to improve the welfare of the individual in question'.¹⁶

Findings from the workshops

Within this evolving context, participants in the workshops identified a number of different rationales for data sharing in order to provide direct benefits to individuals, including:

- **Safeguarding** – protecting an individual's rights to live in safety, free from abuse and neglect.¹⁷ The need to share data for purposes of safeguarding was raised as a key reason for sharing data in all of the workshops.

¹⁶ UK Government (2017) Digital Economy Act <http://www.legislation.gov.uk/ukpga/2017/30/part/5/enacted> (accessed 28/5/2017)

¹⁷ The ability to share the right information, at the right time, with the right people, is fundamental to good practice in safeguarding. The Care Act 2014 therefore permits sensitive or personal information about adults to be shared for safeguarding purposes between the local authority and its safeguarding partners (including GPs and health, the police, service providers, housing, regulators and the Office of the Public Guardian), and allows information to be shared without consent if: the person lacks the mental capacity to make that decision; other people are, or may be, at risk, including children; sharing the information could prevent a crime; the alleged abuser has care and support needs and may also be at risk; a serious crime has been committed; staff are implicated; the person has the mental capacity to make that decision but they may be under duress or being coerced; the risk is unreasonably high and meets the criteria for a multi-agency risk assessment conference referral; a court order or other legal authority has requested the information. Care Quality Commission (2017) Safeguarding People <http://www.cqc.org.uk/what-we-do/how-we-do-our-job/safeguarding-people> (accessed 20/9/2017)

However, as the Care Act places a fixed, non-discretionary obligation on staff to do so in certain circumstances, data shared for the purposes of safeguarding has been excluded from the remainder of these discussions as, given it is a defined professional duty, it is outside the debate about when data should be shared to deliver other public benefits.

- **Sharing case information between services to ensure continuity of care and support** for an individual at points of transition eg patient care plans shared between the NHS and community care providers upon discharge from hospital;
- **Sharing information to enable the right services to be offered to individuals at the right time** eg when the Department of Work and Pensions notifies local authorities and other social landlords when tenants receive Universal Credit so as to allow for the offer of Universal Support;
- **Sharing information to co-ordinate interventions and provide an integrated support service** – Integrated Offender Management programmes wherein probation, police, local authorities, drugs and alcohol services and health providers take a multi-agency approach to supporting and supervising persistent offenders on release from custody to address issues which may contribute to the risk of re-offending, such as drug and alcohol addiction, homelessness, unemployment, health problems and access to state benefits.
- **Connecting the administrative information held about citizens across government departments to simplify and streamline consumer interactions** – reducing the need for citizens to input address and other identifying data multiple times when, for example, applying for a passport, a driving licence and a Blue Badge.
- **Sharing information held by a service to identify people who might benefit from a new, or different, service offer** – a local authority sharing details of those in receipt of

council tax reductions due to disability with their recreation department to enable them to contact residents to promote a new keep fit service for disabled people.

- **Sharing information between services to automatically provide citizens with benefits they are entitled to**, eliminating the need for them to proactively apply for support eg as part of the Government's programme to address fuel poverty, information held by HMRC and the Department of Work and Pensions would be matched with records held by the Department of Energy and Climate Change and the Valuation Office Agency to identify those on the lowest incomes living in the coldest homes so a rebate on their energy bills could be automatically applied.

In most cases, participants in the workshops were very supportive of using data in these ways, viewing sharing arrangements like these as vital tools for enabling public service providers to offer the best possible services to people. The belief was also widely expressed that this is what the public expects from modern services, reflecting evidence from dialogues with the public which showed that they 'commonly assumed that governmental administrative data is already linked and shared across departments, and [that they] supported this for operational uses'.¹⁸ Indeed, the research literature suggests that although most members of the public express opposition when directly asked if they support the use of data held about them being shared, the majority become more ambivalent where they can see direct benefits to themselves from the process.¹⁹

In several of the workshops, participants also went as far as suggesting that public services providers had a lot they could learn from private companies in relation to using data to deliver more bespoke and 'frictionless' services to the public that are 'fit for the 21st century'. This conclusion seems to be reinforced by findings from consumer research

relating to how people balance concerns about how their information may be used when they provide details online. For instance, it showed that '71% of consumers would provide more information online if it helped them save money; 60% would be willing if the resultant service was better tailored to their needs; and 56% would be willing if it helped them to make better decisions'.²⁰



b) Sharing data to deliver benefits to Public Service providers

In a climate in which growing pressure is being placed on limited public-sector resources, governments at all levels have embraced the idea that there is a need for more joined up working to 'modernise' and 'transform' public service provision. The better use of data across and between service providers is increasingly positioned as a vital tool for achieving this goal, by maximising the value of the information being collected by individual services.



'Data is a critical resource for enabling more efficient, effective government and public services that respond to citizen's needs. Data acts as the foundation upon which everything else rests.'²¹

Findings from the workshops

Across the six workshops, participants readily identified situations where having access to more, high-quality information would have made the work of their organisation easier, better targeted and ultimately able to deliver better outcomes for the public. This was, in fact, the dimension of benefit where workshop participants were consistently able to list the greatest range of both short-term and long-term benefits.

Some of the **short-term** / direct benefits to service providers identified included:

18 Ipsos Mori (2014) Dialogue on data: Exploring the public's views on using administrative data for research purposes. Economic and Social Research Council (ESRC). <http://www.esrc.ac.uk/files/public-engagement-public-dialogues/dialogue-on-data-exploring-the-public-s-views-on-using-linked-administrative-data-for-research-purposes/>

19 Davidson, S. McLean, C., Cunningham-Burley, S., and Pagliari, C. (2012) Public Acceptance of Cross-Sectoral Data Linkages. Scottish Government <http://www.gov.scot/Publications/2012/08/9455/0>

20 Coll, L. (2015) Personal Data Empowerment: Time for a Fairer Data Deal. Citizens Advice; <https://www.citizensadvice.org.uk/about-us/policy/policy-research-topics/consumer-policy-research/consumer-policy-research/personal-data-empowerment-time-for-a-fairer-deal/>

21 Cabinet Office (2017) Government Transformation Strategy. UK Government <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020> (accessed 28/5/2017)

- **Reducing duplication and waste** – eliminating instances where the same information is being collected, processed and maintained in multiple databases, thereby freeing up staff resources for other activities;
- **Supporting effective, better targeted front-line service delivery** by providing staff with information from multiple sources to help them make decisions about the support an individual might need, the level of risk they might be exposed to, or whether other organisations should be involved in their case, and thereby better manage cases and caseloads;
- **Directing resource allocation** – by using data from multiple sources to identify crime hot-spots or areas of multiple deprivation to enable resources to be used in ways that will have the most impact;
- **Identifying instances of fraud and/or debt** – maximising revenue generation by using Council Tax records to identify households claiming single person council tax discount where there is more than one registered resident;
- **Monitoring demand and delivery patterns** for different services across agencies to ensure existing models of service provision are making the best use of resources;
- **Improving levels of customer satisfaction** by making the public's interactions with services easier, more streamlined and more likely to deliver a positive outcome quickly and effectively.

Some of the longer-term, strategic and operational planning benefits identified included:

- **Producing local statistics** that maximise the value of existing data to identify, for example, where there is unmet need in the area or where services are not meeting people's needs;
- **Enabling the better monitoring and evaluation of service impacts** – providing evidence that interventions are making a difference in order to appraise options and inform future service planning and commissioning;

- **Facilitating evidence-based policy and decision making** regarding what services are developed and offered to the public, on the basis of rigorously established objective evidence of 'what works', and particularly 'what works' in a local context, speeding up cycles of improvement;
- **Identifying the root causes of problems** by combining multiple data sets about the same people or issues to provide a better picture of the range of contributing factors and improve the accuracy of the diagnosis. This, in turn, helps service providers to identify the best way to both tackle the problem at its source and institute preventative measures;
- **Tracking a service user's journey** to provide longitudinal insight into the experiences of service users and identify opportunities for improvement. For example, one of the case studies used in the workshops illustrated how anonymised linked data had been used to map the interactions a very complex social care client had with the council, and external agencies, over a 10-year period. This provided new insights around the system as a whole and flagged where interventions could have been made earlier to improve care;
- **Predicting future service needs** by better understanding the changing make-up and needs of their client group;
- **Testing strategic and service planning hypotheses** by modelling the impact of new service configurations on resourcing, outcomes and budgets to identify where and how resources can be targeted to have the biggest impact;
- **Developing shared outcomes and indicators across service providers** to support more integrated service delivery practices and increase collaboration.
- **Increasing public trust in government** through the use of data in ways that demonstrated transparency, accountability and wider aspects of good governance.

Overall, participants in the workshops generally expressed high levels of support for using data to enable services to be delivered more efficiently and therefore to support them to 'do more with less'. This sits well alongside research with the public which found one of the main benefits identified from the collection and use of personal data is to assist the Government in 'identifying needs, planning resources and services, and allocating funds'.²²

There was also particular interest in the opportunities created by a more open flow of data between service providers to develop integrated, cross-service performance management frameworks focussed on end outcomes. This was seen as a vital step for demonstrating the impact of 'joined-up' working and evidencing the impacts of co-ordinated activity. There was, however, a degree of hesitancy about whether the wider public would see data being used in for some of these purposes as providing 'public benefits'.



c) Sharing data to provide wider social benefits for people and communities

The idea that data sharing can deliver wider 'public benefit', while regularly cited as an important factor in increasing the social licence for data use²³, is, as noted above, rarely defined further. Instead what these benefits might be in practice tends to be variously glossed over as impacts that are 'in the public interest', 'for the greater good', or 'leading to the improvement of health, education or economic and social well-

being'²⁴. A key goal of the workshops therefore was to dig deeper into what service providers understand these benefits to include.

Findings from the workshops

Across all of the workshops, participants expressed the belief that the effective use of data should be able to deliver wider, positive social outcomes for people and communities (beyond the benefits delivered to individuals and service providers). What these should be, however, was something that participants generally found much harder to articulate.

Three themes did emerge throughout the discussions as being central to the idea of wider public benefit:

- Providing intrinsic benefits to society through access to better public services:** Throughout the workshops it was generally agreed by participants that improving public service delivery overall provided knock-on benefits for all citizens, even if they did not use the specific services. This was largely due to the belief that increasing overall effectiveness, and delivering efficiency savings, would relieve pressure on the public purse.
- Delivering improved outcomes for communities:** Stimulated by the examples presented in the workshops, participants made reference to social outcomes such as improved community safety, reduced social isolation, reduced inequalities and local area regeneration. This aligns with the findings from previous social research which showed that, when directly asked about their expectations relating to wider benefits, the public tended to understand it primarily in terms of improvements to local services, local areas or public health.²⁵

22 Wellcome Trust (2013) Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. Wellcome Trust <https://wellcomelibrary.org/item/b20997358#?c=0&m=0&s=0&cv=0>

23 Ipsos Mori (2016) The one-way mirror: public attitudes to commercial access to health data. Wellcome Trust <https://wellcome.ac.uk/sites/default/files/public-attitudes-to-commercial-access-to-health-data-wellcome-mar16.pdf>; Aitken, M., de St. Jorre, J., Pagliari, C., Jepson, R. and Cunningham-Burley, S. (2016) Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. BMC Medical Ethics 17:73 <https://bmcmethics.biomedcentral.com/articles/10.1186/s12910-016-0153-x>; Sciencewise (2014) Big Data Public views on the collection, sharing and use of personal data by government and companies Sciencewise <http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf>; Ipsos Mori (2014) Public attitudes to the use and sharing of their data. Royal Statistical Society https://www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf

24 Cabinet Office (2016) Better Use of Data – Consultation Paper. UK Government https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/503905/29-02-16_Data_Legislation_Proposals_-_Con_Doc_-_final__3_.pdf; Davidson, S., McLean, C., Cunningham-Burley, S., and Pagliari, C. (2012) Public Acceptance of Cross-Sectoral Data Linkages, Scottish Government <http://www.gov.scot/Publications/2012/08/9455/0>; Open Policy Making Process (2016) Conclusions of civil society and public sector policy discussions on data use in government <http://www.datasharing.org.uk/conclusions/index.html>

25 Davidson, S., McLean, C., Treanor, S., Cunningham-Burley, S., Laurie, G., and Pagliari, C. and Sethi, N. (2013) Public Acceptability of Data Sharing Between Public, Private and Third Sectors for Research Purposes, Scottish Government <http://www.gov.scot/Publications/2013/10/1304/0>

- **Enabling Research:** Providing data for research purposes was also seen as an important aspect of delivering public benefit, even if those benefits may be less tangible and/or not immediately apparent. Previous engagement with the public suggests that they are also cognisant of the value of the long-term impacts that wider social research can enable. A systematic review of 25 studies examining public attitudes towards the sharing or linkage of health data for research, for example, showed that, while individuals receiving direct benefits from research uses of data was important to the public, overall societal benefits were also assessed as valuable, particularly when they were able to demonstrate a ‘real-world . . . practical application’.²⁶

However, it was repeatedly noted that in order to improve public awareness of how data sharing can be deployed to deliver benefits like this, public service providers need to get better at ‘telling the stories’ of how the effective use of data has delivered outcomes for people and communities.

Evaluating the relative value of different benefits

A core objective of this project was to investigate how stakeholders working in different aspects of public service delivery not only understood different aspects of public benefit, but how they valued the different types of benefits the better use of data could deliver. In each workshop therefore, participants were asked to comparatively evaluate a number of examples of data sharing practice, purely in relation to their ability to deliver public benefits. The participants were explicitly asked not to take the risks associated with the initiatives into account when weighing up the relative values of the different benefits.

26 Aitken, M., de St. Jorre, J., Pagliari, C., Jepson, R. and Cunningham-Burley, S. (2016) Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. *BMC Medical Ethics* 17:73 <https://bmcomedethics.biomedcentral.com/articles/10.1186/s12910-016-0153-x>

When individuals were the main beneficiaries

Overall, when workshop participants came to evaluating the comparative public benefits of different forms of data sharing, a key criterion in all locations was the ability of an initiative to deliver clear, demonstrable benefits to individual service users. This corresponds with messages drawn from research with the public which suggest that ‘personal benefit is the strongest incentive for being in favour of the collection and use of personal data by government and companies’ and further that the offer of a specific, tangible benefit has a significant impact on the public acceptability of using personal data.²⁷

 **‘If we could see a benefit to an individual or a life then we saw this as most important.’**
WORKSHOP PARTICIPANT, MANCHESTER

The differences across the workshops, however, were in relation to what type of benefits individual participants valued most highly.

- For some groups, the **number of people able to benefit** from a data sharing initiative was a principle factor for attributing value. Examples that used data to directly identify individuals in need of a specific intervention to improve their wellbeing, or to apply a direct benefit (a rebate or discount), therefore tended to be evaluated highly.
- The perceived **level of need** was another significant factor for some participants. Examples that were seen to have direct impacts on vulnerable groups (eg the homeless) and/or which set out to address key social problems (eg social isolation) were therefore attributed greater value. The degree of positive impact on individuals, and the depth of that impact on their wellbeing, also contributed to participants’ assessments. As

27 Sciencewise (2014) Big Data Public views on the collection, sharing and use of personal data by government and companies Sciencewise <http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf>

one group from the workshop in Manchester noted, they made their evaluation based on the *'level of need of beneficiaries, the urgency of the problem and the level of positive impact it would have on beneficiaries'*.

- **Long-term impacts** on the services available to people was also seen by some groups as a critical criterion. In these cases, examples that demonstrated how large-scale, linked data sets could be used to both monitor service performance and identify which services would be most beneficial to individual users were particularly valued. Examples that used large aggregate data sets to identify trends (eg areas of multiple deprivation) and provide evidence for targeting resources differently, were also seen as able to provide benefits to large numbers of people in the long term.

'Using data well now can mean future service users get a better service – or even don't need the service.'

WORKSHOP PARTICIPANT, SHEFFIELD

When Public Service providers are the main beneficiaries

When organisations and service providers themselves were seen to be the sole, or primary, beneficiary from a data sharing initiative, participants tended to assess this scenario as having lesser public benefit value, expressing concerns about whether the public would see this as an acceptable use of the data held about them. In contrast, when service providers were identified as being one among a number of potential beneficiaries from a data sharing initiative, support for the initiative's ability to deliver public benefit significantly increased.

Of the different types of benefits that could be accrued by public services, participants ranked the following four most highly:

- The ability of data to be used **to help inform resource allocation**. Examples that allowed service providers to make efficiency savings by more effectively allocating staff and resources were generally seen as producing wider benefits, by freeing up scarce public-sector resources for other uses, and thus ranked highly. Examples that had the potential to impact on long-term service planning and efficiency, by using data to monitor patterns of service use, predict future demand and identify opportunities for innovation, however tended to be ranked even higher.
- When the use of data enabled service providers **to produce evidence of 'what works'**. For instance to evaluate the impact of interventions, demonstrate value for money and inform future service design in ways that would ultimately improve outcomes for service users then this was seen to deliver wider public benefits. This led to examples like the Justice Data Lab being assessed as very beneficial. In this example, organisations working with offenders would share information about their participants with the Ministry of Justice. The MOJ then compares rates of re-offending among participants in these programmes with re-offending rates among a matched control group to provide the organisation with information they can use to evaluate the effectiveness of a specific intervention.
- Examples that were designed to use data to **identify the underlying causes of social problems and reduce the need for crisis services** in the future were also highlighted. These types of examples were viewed by many as having the ability to inform strategic service changes in ways that could have significant impacts on both public service providers and community wellbeing in the future. As participants in the workshop in Melton Mowbray noted: *'If you reduce need, you reduce costs!'*
- When data was used to enable a more **holistic approach to service provision**, through integrated working and sharing information across multiple service providers then these initiatives were also favoured, for

example, using data to track service users' journeys in ways that could inform long-term improvements in when and how services are offered and delivered.



When the wider public is the main beneficiary

As already noted, the importance of the wider public being a beneficiary from the use of data was seen as vital for obtaining social licence for the greater use of data. This seems to resonate with the research that shows that, while personal benefit is the strongest incentive for members of the public being in favour of the collection and use of personal data, it is closely followed by 'public goods' (health improvement, prevention and detection of crime, and the detection of fraudulent behaviour).²⁸

Examples that participants believed could generate positive social outcomes (rather than simply benefits to individuals and/or service providers), therefore tended to be evaluated most highly in terms of delivering public benefits.

- A key criterion across most of the workshops was the ability of an initiative to have **positive impacts on multiple types of beneficiaries**, such as individuals, services and the wider public. The example of the integrated database for Health and Social Care providers in Hertfordshire was highlighted as archetypal in this regard: able to provide

²⁸ Suherman-Bailey, J. (2015) Data policy and the public: shaping a deeper conversation. Sciencewise <http://www.sciencewise-erc.org.uk/cms/assets/Uploads/Data-policy-and-the-publicJan-2015.pdf>

benefits to individuals (by ensuring patients were offered appropriate services at the right time); to staff (by enabling more efficient and co-ordinated working); and to services as a whole (by increasing their ability to monitor performance, evaluate impact and use this information to inform service planning). This type of approach to data sharing was assessed as having clear public benefits in the workshops, as it was seen to have the potential to deliver cumulative impacts across services and wider society.

- In a number of the workshops, participants used the criterion of **positive social outcomes** to rank highly examples that focused on addressing fundamental social problems (like social isolation, violence in communities and homelessness). When data was used to undertake social research, for example into the impacts of poor housing on long-term health, these were also rated highly for providing evidence that could be used to deliver wider social benefits if applied to policy making.
- Improving the **effectiveness and efficiency of public service provision** overall was also seen as a 'win-win,' benefiting individuals, public agencies and the wider public. These types of benefits were variously described across the workshops as the 'knock-on' or 'ripple effects' of a data sharing initiative. They included outcomes such as increased partnership working, efficiency savings decreasing demands on the public purse and reduced need for services due to early intervention.

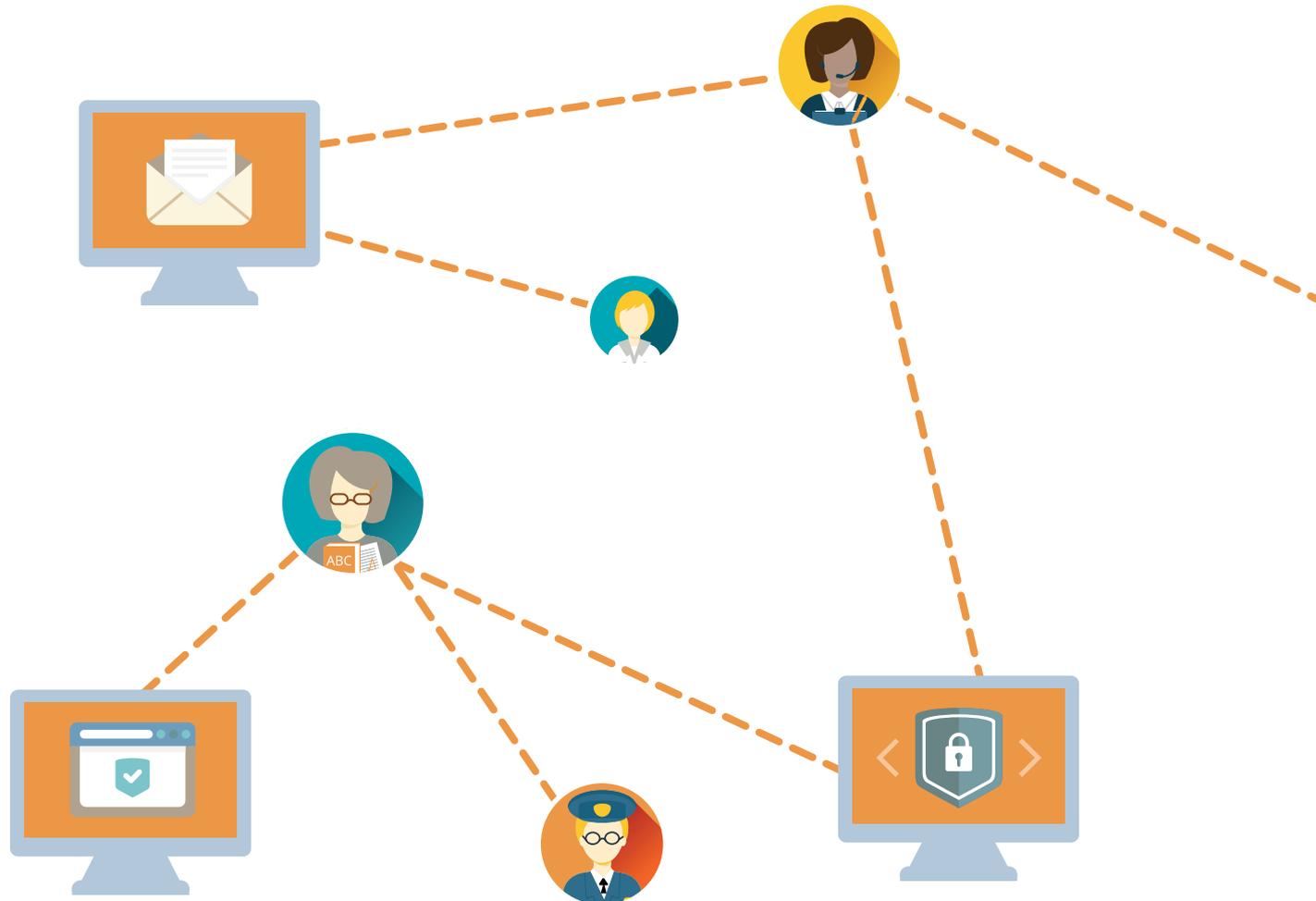


Conclusions following the workshop process

Across all of the workshops, participants were easily able to identify a range of opportunities for increased data sharing in their own work or organisation and recognise the positive impact that the continued development of data use across their local area could make to service delivery. When it came to being able to articulate the wider public benefits that the better use of data could deliver, participants generally had more difficulty.

Importantly, it also became apparent very early in the process that public service providers do not have anything approaching a common framework to draw upon in order to identify, classify or evaluate the benefits that data sharing may be able to provide. This was found to be equally the case in areas where there was already a strong leadership commitment and resource investment in improving how data is being shared, as it was in areas where processes were less developed.

This lack of consistency in the way the potential benefits from using data are understood and evaluated has a direct impact on what different stakeholders consider to be beneficial uses of data. This also has clear implications for how service providers perceive and assess the risks associated with greater data use, as discussed in the next chapter of this report.



4. Identifying Dimensions of Risk

Whenever personal data is collected, accessed, analysed, shared or linked there is some risk to individual privacy. Much of the current debate around when personal data about service users and the wider public should be used to support the better delivery of public services has therefore focussed on whether data can be used in ways that protect and enhance privacy, while still enabling service providers to maximise value for service planning and delivery.

In framing this research, our initial focus was on determining how professionals working across the public and the voluntary sectors identified and assessed the risks to privacy that the increased use and sharing of data might entail: with a particular focus on how issues such as the type of data shared; levels of informed consent; and the type and number of organisations data was shared with impacted upon assessments of risks to privacy. Throughout the workshops, however, it quickly became apparent that individual privacy was only one dimension of risk that participants considered when identifying the potential harm that a data sharing initiative may cause – to individuals, communities and services themselves.



a) Risks to individuals from the use of personal data

Previous research exploring public attitudes towards public sector data sharing suggests that a key concern for most people is whether the information would be personally identifiable.²⁹ In most cases, it seems that people intuitively understood this to mean whether their name, address or another unique identifier like NHS number or National Insurance number would be disclosed. However, as Understanding Patient Data's work on the Spectrum of Identifiability³⁰ demonstrates, the lines

between what counts as personally identifiable data and anonymised data are not that clear cut.

Fundamentally, in order to achieve the types of benefits outlined in the previous sections, the information that agencies would need to share about individuals is likely to include a wide range of personal data, including potentially sensitive personal data. It could include information supplied for the purposes of claiming benefits, personal medical or financial information, or records demonstrating eligibility for support services like counselling or housing assistance. In short, information that many people would consider, and want to keep, private.

When services use this type of information, it has the potential to create a range of risks, and indeed perceived harms, to individual data subjects. A range of dimensions of risk were identified across the workshops.

- **Incursions into privacy from the use of identifiable personal information:**

Unsurprisingly, participants in the workshop were most comfortable with personal data being used when it was shared in anonymous, aggregated forms, assessing this as posing a minimal risk to individual privacy. This aligns clearly with findings by the Economic and Social Research Council which showed that 61% of the public did not care how their personal data was used, as long as it was anonymised and could not be linked back to them.³¹

Participants were also generally comfortable

29 Aitken, M., de St. Jorre, J., Pagliari, C., Jepson, R. and Cunningham-Burley, S. (2016) Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. *BMC Medical Ethics* 17:73 <https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-016-0153-x>; Davidson, S., McLean, C., Treanor, S., Cunningham-Burley, S., Laurie, G., and Pagliari, C. and Sethi, N. (2013) Public Acceptability of Data Sharing Between Public, Private and Third Sectors for Research Purposes, Scottish Government <http://www.gov.scot/Publications/2013/10/1304/0>; Wellcome Trust (2013) Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. Wellcome Trust. <https://wellcomelibrary.org/item/b20997358#?c=0&m=0&s=0&cv=0>

30 Annex B Understanding Patient Data (2017) What are the best words to use when talking about data <https://understandingpatientdata.org.uk/what-are-best-words-use-when-talking-about-data>

31 Ipsos Mori (2014) Public attitudes to science. Department for Business, Innovation and Skills (BIS) and the Economic and Social Research Council (ESRC). <https://www.ipsos.com/ipsos-mori/en-uk/public-attitudes-science-2014>

with de-personalised linked data being used within a particular service, or as part formal partnership arrangement, to enable service improvements, monitor impact and/or inform organisational strategic planning. This position appears to align with public attitudes research that showed ‘there was near universal acceptance of public bodies’, including the Government, the NHS, local authorities and the police, having access to anonymised personal data from other organisations for research and planning purposes.³²

Views toward sharing personally identifiable information were generally more mixed, with health information highlighted as being particularly private, sensitive and open to misuse should they be disclosed inappropriately. In several of the workshops, however, participants did question whether the potential negative impacts of this were any more significant or damaging to an individual’s wellbeing and life chances than the disclosure of other forms of personal data, particularly data relating to interactions with the criminal justice system or financial and/or benefits records.

Overall, however there was a general consensus among participants that public services should avoid sharing the information they held in personally identifiable forms unless the objectives of the initiative could not be met without it.

- **Risks from insecure data management and storage:** Uncertainty about whether personal data can, in practice, be securely collected, stored, shared and used invokes an inherent risk to individual privacy and has major implications for whether or not agencies and individuals are supportive of data sharing. While technical debates regarding whether it is possible to guarantee the security of information sharing technologies were explicitly placed outside the scope of this project, the impact that these concerns have on attitudes to data sharing are real and justified and were raised during all of the discussions.

Across the workshops, most participants agreed that compliance with regulation, strong controls on who is able to access personal information and good data sharing governance practices should be able to ensure that security risks associated with a data breach or loss, or the intentional misuse of data were minimised.

- **Risks from unintended re-identification:** While the use of de-personalised linked data was recognised as a valuable tool for service providers, and broadly supported by participants in the workshops, they were generally less comfortable with de-personalised data being shared when the data sets were small, as it was feared that this increased the likelihood of re-identification. An example of an A&E department which routinely shares de-personalised patient information related to violent crime injuries with the Community Safety Partnerships (about the time, date and location of the incident and the primary means of assault ie weapon or body part used) in order to allow police to identify and target violence hot-spots, raised particular concerns in this regard. It was considered to be a situation in which the potential re-identification of individuals may be likely and also that the impact of re-identification would represent a significant potential cost to the individual by making them vulnerable to punitive consequences, such as punishment from the police and/or from others within the community.
- **Exposure to unwanted attention / service offers:** When personally identifiable information is shared between agencies, particularly without the direct consent of the individual, this could expose individuals to unwanted or inappropriate offers of service. Participants worried that this could result in harmful outcomes for individuals if they became hesitant about accessing necessary services due to concerns about how the information they provide may be used.

32 Davidson, S., McLean, C., Treanor, S., Cunningham-Burley, S., Laurie, G., and Pagliari, C. and Sethi, N. (2013) Public Acceptability of Data Sharing Between Public, Private and Third Sectors for Research Purposes, Scottish Government <http://www.gov.scot/Publications/2013/10/1304/0>

- **Punitive impacts:** Across the workshops, data sharing initiatives that identified individual cases of fraud, error or debt received a mixed response from participants, particularly when data about individuals was used in ways people were unlikely to expect (for example matching properties receiving an Empty Homes Council Tax discount with credit card registrations to identify lived-in properties). While civil society campaign organisations working in this area tend to argue that ‘it is unethical for improvements in technology for collecting and analysing data to lead to sanctions for individual citizens, even if an argument around the wider public benefit can be made’³³, conclusions drawn from research with the public on this matter appear contradictory. Some studies have shown that the public were broadly supportive of data being used to unearth dishonesty (for example with 72% agreeing that tax and benefit records should be used to prevent fraud)³⁴ while others have concluded that the public are very concerned about data being used by the Government to punish or withdraw a benefit or service from individuals.³⁵



b) Risks to communities and the wider public from the use of personal data

Just as the better use of data may have the potential to deliver benefits to communities and the public, there is also a risk that data can be used in ways that have negative impacts on specific areas or groups. Opportunities for potential harm identified in the workshop are summarised below.

- **Stigma and discrimination:** Concerns were raised that sharing and linking data for the purposes of targeting public services, even if the information used was not personally identifiable, could result in the production of generalisations that categorise individuals,

33 Open Rights Group (2016) Consultation Response Data Sharing <https://www.openrightsgroup.org/ourwork/reports/orgs-response-to-data-sharing-consultation>

34 Ipsos Mori (2014) Public attitudes to the use and sharing of their data. Royal Statistical Society https://www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf

35 Wellcome Trust (2013) Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. Wellcome Trust. <https://wellcomelibrary.org/item/b20997358#c=0&m=0&s=0&cv=0>

social groups or geographic areas in ways that could result in stigma. The example referred to above, where information about violent assaults was shared between A&E departments and Community Safety Partnerships, proved to be particularly contentious in this regard. While participants recognised and valued the public safety benefits that an initiative like this could bring, many felt that the potential negative impacts on communities from being identified as ‘*violent hot-spots*’ or as areas in need of additional police attention could lead to discriminatory treatment or inappropriate targeting. This reflects fears raised by the public during consultations related to the Connected Health Cities initiative, where one of the main concerns raised by the citizen jurors was that the proposed use of data ‘may lead to an increase in geographic, community-based, and social stereotyping and stigmatisation as well as an inequitable distribution of resources’, in other words a ‘postal code lottery’ in relation to service provision across different areas.³⁶

- **The potential for negative impacts on communities from the selective use of data:**

Concerns were raised during the workshops that the selective use of data (particularly without wider qualitative or contextual information) could result in erroneous or questionable conclusions being drawn. This was particularly considered to be a risk where data was being used to develop evidence for advocacy or targeting resources differently. The example where data from the index of multiple deprivation was combined with records showing patterns of GP use to argue for new models of funding GP surgeries in deprived areas, was cited as a case where data might be selected to confirm a pre-existing hypothesis. Participants suggested that if either different data was used, or an alternative approach taken to analysis, the data might ‘*tell a different story*’.

- **Loss of services:** just as the better use of data may be able to support agencies to

36 Citizens Juries c.i.c (2017) Connected Health Cities Citizens’ Juries Report. NHS A <https://www.connectedhealthcities.org/wp-content/uploads/2016/08/CHC-juries-report-Feb-2017.pdf>

more effectively allocate resources on the basis of areas of greatest need and evaluate the demand and performance of different services, it can also be used to reduce or remove services from areas or communities. While these decisions may be evidence based, they can still lead to legitimate feelings of loss among the communities affected.



c) Risks to public service providers from the use of personal data

The participants in the workshops identified a number of risks to service providers that they felt needed to be considered alongside risks to individual privacy if ambitions for the increased use of data to inform service provision were to be realised.

- **Legal risks associated with data loss or misuse:** Participants in all of the workshops noted that this was a perennial concern for service providers when it came to using personal data. While, as noted above, there was general agreement that effective data management controls could minimise the risk of unintentional loss or disclosure, there remained concern that lack of awareness or malicious acts still had the potential to expose an organisation to significant risk.
- **Loss of public trust from using data without consent:** As noted in the introduction to this report, public authorities are permitted to share information without the consent of the data subject through a wide range of legal gateways. For many participants in the workshops, the fact that a data sharing initiative may be legally compliant was very often not enough to assess it as being of low risk. Instead, public expectation was considered a significant factor, with participants tending to make their judgement based on whether a proposed use of data was something that the public was likely to be aware of or could reasonably expect. This led to some of the examples considered that used data without consent being assessed as high risk for service providers, even if they were compliant with the principles of the Data Protection Act.

- **Reputational risks from using sensitive personal data:** The Data Protection Act recognises some forms of personal data as being particularly sensitive, and of a particularly private nature, because information about these matters could be used in a discriminatory way.³⁷ In the workshops, financial and health data were highlighted as being particularly sensitive forms of data that service providers are often especially cautious about using.

One example discussed was the new powers granted to government in the Digital Economy Act to share identifiable tax credit information about citizens with licenced energy suppliers so that companies can automatically apply a 'Warm Home' rebate or offer support under Energy Company Obligation schemes. This was considered by many as a significant incursion into privacy. Participants tended to agree that since it was unlikely that most people would expect this type of financial information about them to be shared without their explicit consent, the risk associated to organisations through the use of this type of data was heightened.

“the standards for demonstrating public benefit have to be seen as higher for some areas of public policy where the possible harm caused by the intrusion is higher.”

WORKSHOP PARTICIPANT, WEST MIDLANDS

Although health and care data was also identified as being particularly sensitive, it was also noted that the public generally expect this type of information to be shared between service providers who are involved in supporting their wider wellbeing (and often assume that it is shared more widely than it usually is in practice). The perceived acceptability of sharing this information within a context of providing direct care, despite its sensitivity, aligned clearly with findings from research with

³⁷ Sensitive Personal Data is denoted in the Act as being information related to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexuality and criminal justice history, and there are provisions within the Act to ensure that personal information of this type is treated with greater care than other types of personal data. UK Government (1998) Data Protection Act <https://www.legislation.gov.uk/ukpga/1998/29/contents> (accessed 28/5/2017)

the public which showed there is ‘a perceived unquestionable benefit to people in terms of experts having information about their health, in relation to illness or avoiding it’.³⁸ When workshop participants were discussing examples of personally identifiable health data being shared outside a direct care context (for example with police or housing authorities) they tended to express more caution, arguing that the impacts of it being disclosed, lost or otherwise misused could be very significant for individuals, and result in significant reputational damage to service providers.

- **Risks from sharing data with organisations outside the public sector:** Across the workshops, a number of the examples presented involved data sharing between the public and voluntary sectors and/or with private companies. Overall, there was very little objection raised to the principle of sharing data with the voluntary sector and in fact, it was widely seen as increasingly necessary in order to enable effective partnership working. However, it was acknowledged that the public may not expect their information to be shared in this way.

The intuitive response to data sharing with the private sector from many workshop participants was that it posed a significant risk, as they did not trust commercial organisations to behave responsibly with data. However, participants tended to become more accepting when they considered the reality that any data sharing arrangement between a public body and a private company would likely be based on a contractual arrangement to deliver services and have strict data use controls in place.

Overall, however, in relation to sharing public sector data with the voluntary or private sector, it appeared that workshop participants’ evaluation of risk rested more on the potential for gain in terms of likely derived benefit, and on the process and controls in place to mitigate data privacy risks, than the type of organisations the data was being shared with.

- **Using data for purposes that are not publicly acceptable:** Concerns were also raised during the workshops that uses of data that primarily benefited service providers – particularly uses that had punitive impacts on individuals – may not be considered an acceptable use of personal data by the public. This nervousness was particularly apparent in response to the one of the case studies used in some of the workshops – the Camden Residents Index which brings together data from 16 council business systems, covering 123 fields of primarily demographic information, to create a complete picture of each resident in order to streamline Council processes and residents’ interactions with services. Here, participants were especially concerned about how the public would evaluate this model of data sharing as the benefits identified were predominantly for the service provider itself (eg validating residency for accessing council services such as school places), and included punitive impacts for individual residents (eg flagging cases of illegal subletting). Overall in this case, while participants could recognise the benefits to a local authority of this type of systematic internal data sharing, many remained nervous about how an initiative like this would be perceived by the public.
- **Risks to service provision from the use of unreliable data:** participants identified that there were significant risks to service providers, and ultimately to the services provided to the public, if flawed or incomplete data was used to inform policy decisions or resource allocations. Participants in many of the workshops recognised that public service organisations do not always have effective and reliable mechanisms in place to collect the right types of information, categorise it consistently and update it regularly – noting that ‘*any system is only as good as the data you put in*’. This created a nervousness that services using data to inform decisions might be relying on unreliable or potentially out of date information.

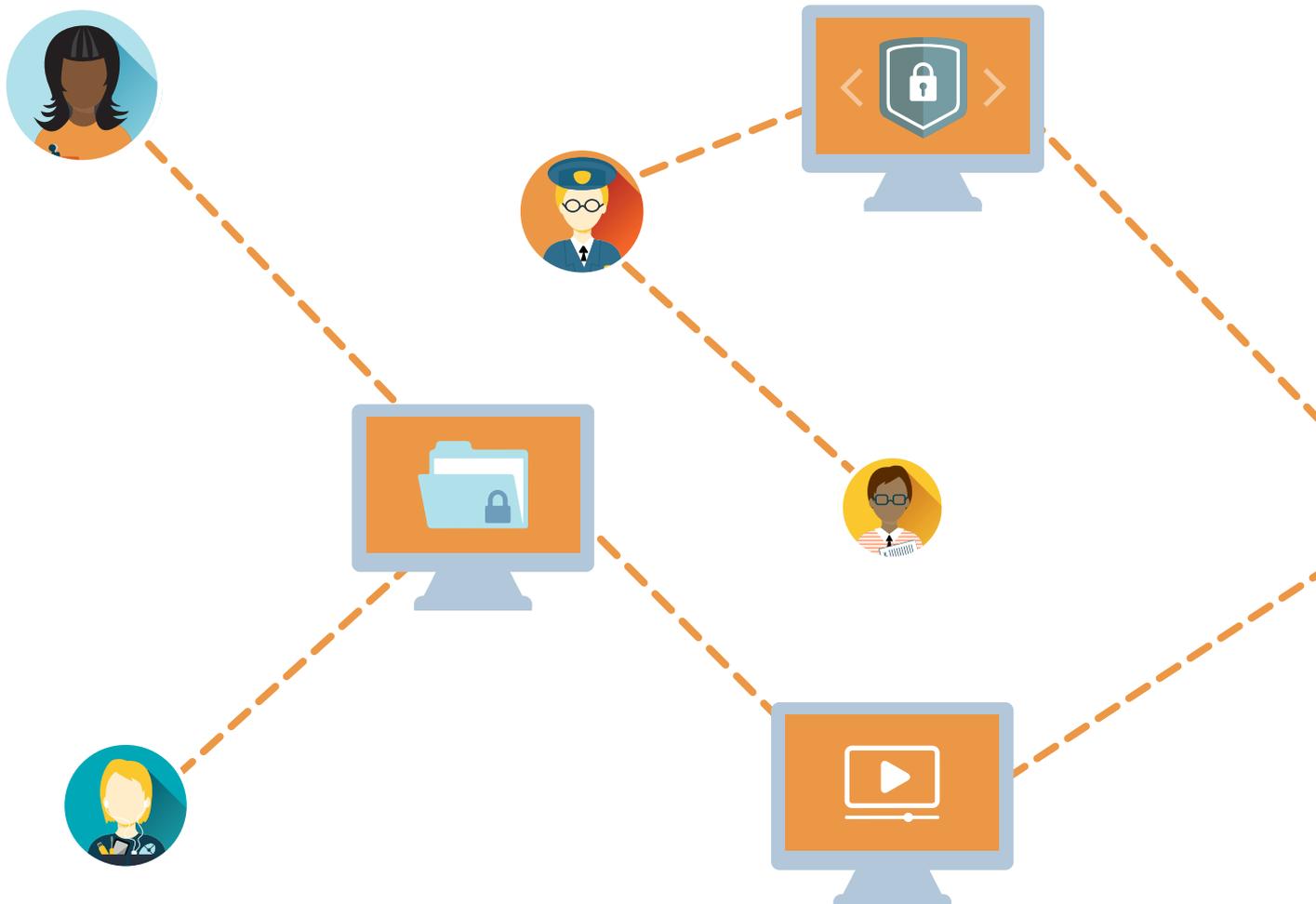
38 Wellcome Trust (2013) Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. Wellcome Trust <https://wellcomelibrary.org/item/b20997358#c=0&m=0&s=0&cv=0>

Conclusions following the workshop process

Throughout the workshops, participants from both the public and voluntary sectors identified a wide range of potential risks from sharing and using data to deliver improved public services. The risks they identified were far wider than the risks to privacy which currently dominate the debate about data sharing. This suggests that there is a need for a renewed, and deeper societal debate to understand the extent to which the public share the same concerns and where the deepest public disquiet lies.

It was also very clear that as in the case of assessing and evaluating potential benefits, professionals working across these field have no common framework for attributing risk when considering potential data sharing initiatives. Instead, as many participants readily admitted, the default position they adopted in practice was one of caution and restraint.

In the next chapter, we explore how participants went about balancing the risks and benefits related to different examples of data sharing practice when challenged to assess the relative acceptability of a potential data sharing initiative.



5. Determining acceptable uses of data to deliver Public Benefits

It is clear from the previous chapters that there are tensions between expanding opportunities for data sharing, protecting privacy and mitigating the wider risks associated with sharing personal data. It cannot be assumed that these are entirely compatible goals.

Finding an acceptable settlement between the use of data to deliver services that benefit the public and protecting people's privacy therefore remains a key challenge for policy makers, frontline staff, advocacy groups and the public at large if the ambitions for data to be used as a tool for delivering public benefit are to be realised.

Principles for assessing public benefit

Discussions during the workshops raised a range of issues related to appropriate purposes, groups of beneficiaries, types of data being shared, and the privacy incursions and associated risks that need to be identified, acknowledged and weighed up before the relative acceptability of different forms of data sharing to deliver public benefits can be determined. Three clear principles, however, emerged throughout the workshops as being necessary conditions for public service providers to gain the social licence to share and use data more widely based on the promise of delivering public benefits: purpose, proportionality and responsibility.

The remainder of this chapter looks at each of these principles in turn and presents the various factors participants weighted up, as well as the types of questions they debated, when assessing the potential value of an initiative. Presented in order of the frequency and intensity in which they were emphasised across the workshops, this provides a cumulative map of the factors that were considered most important in determining acceptable use of data to deliver public benefits.

That data use should be purposeful

When the purpose of a proposed use or sharing of data is clearly defined, and presented transparently, participants more readily accepted it. Across all of the workshops, there was a general resistance to data being shared and/or linked for speculative purposes or 'fishing expeditions', as this was felt to be one of the quickest ways to lose public support for the use of data held about them. It was also argued that clarity and transparency of purpose helped provide protection (for both the data subject and the organisations involved) against data being used for purposes beyond that for which it was initially shared.

Additionally, for a use of data to be accurately described as delivering 'public benefit', workshop participants tended to agree that it needed to be geared towards a publicly acceptable purpose. There were, however, a wide range of opinions expressed as to where the boundaries of public support would lie, ranging from undisputed 'social goods' like improved community safety and public health at one end of the spectrum, to preventing fraud and maximising public sector revenue by enabling punitive action to be taken against individuals at the other. This suggests that there is a need for further direct engagement with the public to better understand where their boundaries of acceptability lie within the context of data sharing.

A number of additional factors impacted on participants' assessments of the acceptability of purposes geared towards delivering public benefit:

- **That the use of data provides direct and tangible benefits to individuals.** Delivering demonstrable benefits to individuals' wellbeing was identified as an important criterion for assessing an initiative as delivering 'public benefit'. It was also acknowledged however, that in many cases, the uses of data that have the most potential to directly benefit individuals were those that also involved the greatest incursions into individuals' privacy (and thus also presented the greatest reputational risk to service providers). While gaining the consent of individuals for data about them to be shared was universally seen as the best way of overcoming these concerns, it was also recognised that this was not always feasible.

When considering the acceptability of data shared without consent, in order to directly contribute to an individual's wellbeing, key questions participants asked themselves were:

? *In what circumstances does the benefit offered outweigh the incursion on privacy? Are there circumstances in which the use of personal data without consent presents such a minimal harm to an individual's privacy that the incursion is justified?*

- **That the use of data delivers positive social outcomes.** When data sharing initiatives were seen as capable of exerting a measurable, beneficial impact on the lives of people and communities (eg through reduced social isolation, reduced inequalities and local area regeneration), then these uses were generally seen as being more acceptable than when data was used for punitive purposes.

Key questions participants asked themselves when considering this were:

? *Is the way data is shared and used making a direct contribution to these outcomes? Would the public recognise these outcomes as acceptable uses of data held about them? At what point do initiatives that may benefit the majority, but have the potential to have a negative impact on other sectors of society, become unacceptable?*

- **That the use of data impacts on multiple beneficiaries** such as individuals, services and the wider public. The acceptability of data sharing activities was seen to rise if the use of data was able to advantage multiple beneficiaries. The likelihood of 'knock-on' or 'ripple effects' increased acceptability, as did the ability to maximise these benefits in long-term, sustainable ways.

The key questions that participants asked themselves when seeking to determine whether a use of data could be justified on the basis of providing multiple benefits were:

? *Who are the beneficiaries of this exercise and how much, proportionally, do they benefit? How ready are the public to recognise uses of personal data that appear, particularly in the short term, to primarily benefit service providers as delivering wider public benefits?*

- **That the purpose aligns with what the public would expect.** This was considered to be a significant factor in determining the acceptability of data use in the majority of the workshops. Participants recognised that this is challenging, given that the public may not have a clear understanding of the opportunities that the data held about them might offer for informing service improvements, or have a defined expectation of how data may be productively used by service providers. However, it was seen as important to maintaining public trust that service providers did not overstep the boundaries of what the public could reasonably expect data they had provided to be used for.

The key questions that participants asked themselves when assessing whether a potential use of data would be acceptable included:

? *How aware are the public that data held about them could be used for secondary purposes? Is it reasonable to expect that data collected by public service organisations may be used for this purpose? Was the information initially provided in a context in which the public would expect it to be kept confidential?*

- **The nature of the problem being addressed.** As noted earlier in this report, some types of social problems were seen as more important, and more difficult and complex, to address than others eg homelessness, violence in communities and social isolation among the elderly. Some participants considered that if a data sharing initiative had the potential to address a significant social problem or provide life-changing benefits to vulnerable individuals or those suffering from multiple disadvantages, then even in cases where this might entail significant incursions into an individual's privacy and/or result in the loss of service users' trust, this could be considered an acceptable risk and therefore an acceptable use of data.

Key questions participants asked themselves in this context were:

? *Are the potential benefits to individuals worth breaching individual privacy? Can this problem be addressed better without sharing personal data? Will wider society, if not the individuals involved, accept this type of activity as one delivering public benefits?*

'We can mitigate the risks but we can't change the benefits.'

WORKSHOP PARTICIPANT, MANCHESTER

- **That the use of data achieves long-term impacts.** While recognising that the better use of data can deliver immediate benefits to individuals, in some of the workshops, participants tended to attribute more value to examples that were able to deliver long-term, systematic or strategic benefits. This included benefits that were likely to apply mainly to future, rather than current, service users. When data sharing initiatives were assessed as addressing the root-causes of problems (for individuals or in relation to wider

social issues) perceived acceptability tended to increase, regardless of the potential impact on individual privacy. This was in part due to a belief among participants that unintended negative consequences were more likely to emerge when initiatives were primarily reactive or 'plastered over' symptoms of a bigger problem.

When attributing value to a potential use of data using this as a criterion the key questions that participants asked themselves were:

? *Is this use of data getting to the root cause of the problem or addressing its symptoms? Can it contribute to long-term social change? Is the short-term risk to services from using data in this way worth the long-term gain?*

- **That the use of data minimises negative effects.** We noted earlier that, alongside any benefits they may offer, many potential uses of data by public service providers may result in negative consequences (intended or unintended) for individuals and groups, for instance through excessive incursions into privacy; punitive action; the risk of stigmatisation/discrimination; or the diversion of resources from one area/sector of the population to allow focus to be given to another. At some of the workshops, this was a central consideration for participants when assessing the acceptability of opportunities for data sharing.

Key questions participants asked themselves in these cases were:

? *Do any potential negative consequences outweigh potential benefits? Are there ways to minimise negative effects? If not, are the expected benefits to individuals, groups within society or services themselves worth accepting the negative public response that may result?*

✓ *That data use should be proportional relative to its intended outcome*

There were a number of factors that contributed to assessments of proportionality across the workshops:

- **That the data use minimises the amount of data shared.** Concern was expressed that when a large number of data sets are linked, this increases the risk that data subjects could be re-identified. In other cases discussed, the sheer number of data sets involved began to feel to some participants like an instance of doing this ‘because we can’ rather than ‘because it is needed’.

The key question participants asked themselves when assessing whether proposed uses of data were proportionate was:

❓ *Is all the data shared/linked strictly necessary for the intended purpose?*

- **Whether there is a need for personally identifiable data to be shared in order to achieve the intended outcome.** Whether the data used needed to be personally identifiable was highlighted as a central consideration in determining proportionality and ultimately, acceptability. It was widely agreed across all of the workshops that data should be anonymised by default, unless there was a clear and valid reason for it to be personally identifiable.

Key questions workshop participants asked themselves when determining whether a proposed use of data was proportionate were:

❓ *Is the data being shared personally identifiable? Does it need to be? Would there be another way of achieving the desired outcomes without using personally identifiable information?*

- **Clear parameters for data use.** A central factor in assessing the acceptability of the sharing of personal data was that there should be clear boundaries in place regarding who is able to access it and for what purposes. This was generally considered to be a valuable protection against ‘mission creep’ and the risk

of data being used for purposes other than that for which it was provided or shared.

Key questions participants asked therefore when assessing whether proposed uses of data seemed proportional were:

❓ *Are there clear restrictions on what this data can be used for? Are the people who have access to the data aware of these limitations? Is access, particularly to personally identifiable data, restricted to a ‘need-to-know’ basis?*

- **The likelihood of risks being realised.** While a number of potentially significant risks to individual privacy and to the reputation of service providers were identified during the workshops, many participants felt it was important to balance the severity of the impact with the likelihood of it happening. There was a general sense across most workshops that well conceived, well designed and well governed data sharing initiatives should be able to mitigate against unintended consequences, thus minimising the likelihood of potential risks being realised. It was also proposed that the existence of risk should not automatically discount an opportunity being pursued if there was significant potential to deliver public benefits. On this basis the key questions participants asked themselves when considering the proportionality of risk were:

❓ *How likely were potential negative impacts? How confident were they that the risks associated with a particular use of data could be effectively mitigated? On balance, was the proposed use still desirable?*

- **The sensitivity of the data being used.** Although the type of data shared was discussed as a factor in assessing risk, when it came to concluding overall acceptability through balancing up risks and benefits, this was not a principal consideration for most participants. Instead, it was widely held that the purpose of the data sharing should be allowed to define the type of data that was needed.

Key questions that participants asked themselves when considering the use of personally sensitive data were:

- ?** *Is this specific type of data needed to achieve the identified purpose?*
- Are there any particular reasons to consider this type of data more sensitive than other forms of data in this context?*
- Are there sufficient protections in place to minimise the risk of harm to individuals from the use of this type of data?*

✓ The responsibility of data uses

To be a justifiable use of public resources, participants noted that the benefits likely to be achieved by a particular use of data have to be balanced against not just the risks, but the overall ‘costs’ involved in delivery.

‘The benefits achieved by the use of data have to outweigh not just the risks, but also the effort, time, financial outlay, resources and opportunity costs involved.’

WORKSHOP PARTICIPANT, SHEFFIELD

A variety of factors were identified within the workshops that contributed to assessments of whether a particular opportunity for data sharing could be considered an efficacious use of public resources:

- **That it is a ‘good’ use of data.** When this was adopted as a criterion for assessment, the discussion focused both on the quality of the data (in terms of accuracy and timeliness) and whether the use of personal data (given known public concerns around how data about them was used) added significant value to decision making or policy implementation. Participants also noted that there was a need for caution in relation to the increased reliance on quantitative data as a ‘catch-all’ solution for improving public service provision, stressing instead that access to data about service users was only one source of intelligence

available to service providers. However, when using personal data was assessed as being able to deliver benefits in a more efficient and effective way than other approaches, its acceptability increased as an approach deserving of public investment.

Key questions that participants asked themselves were:

- ?** *Is the data service providers have access to reliable, complete and timely? Is the use of personal data about service users or the wider public the ‘best’ way to achieve the desired ends?*

- **That data can be used and shared securely.**

Alongside purpose and proportionality, the processes involved in data sharing and use are also vitally important for assessing acceptability. Workshop participants believed there needed to be consideration of ‘*the how, not just the why*’ in any assessment of potential data uses. The ability to give an unequivocal response to public questions relating to how data was being used, including a clear statement of the storage and processing procedures, access restrictions and the controls in place to protect individual privacy, was seen as vital to extending service providers social licence to use data in new and different ways to improve service planning and delivery.

‘Fears about security and risk shouldn’t be a barrier for good projects that have potential; we just need to be clear about the safeguards we put in place to mitigate risks.’

WORKSHOP PARTICIPANT, LEEDS

Key questions that participants asked themselves when considering risks to data security were:

- ?** *Are the proposals fully compliant with current data protection regulations? Are there sufficient data governance procedures in place to ensure that security risks are minimised? What more could be done to mitigate security and/or privacy concerns?*

- **That the use of data will deliver the intended outcomes.** Here discussions tended to focus on whether there was confidence that the proposed use of data sharing would be able to deliver the benefits intended.

Key questions that participants ask themselves when considering this were:

? *Does the hypothesis underpinning the rationale for data sharing ‘ring true’? Does using data in this way expose an organisation to additional risks if the expected benefits from the use of data are not realised?*

- **That the use of data is justifiable.** In the workshop discussions, it was recognised that the public and service providers (and even different branches of the public sector) are likely to evaluate the risk/benefit trade-off differently depending on their own priorities. It was felt that this was particularly likely to be the case when the beneficiaries may not be the ones shouldering the risks: for example, if the risk is to individual privacy, but the benefit is to service provider efficiency, or alternatively, if the benefit is to vulnerable service users, but the risk relates to wider public trust in how services use the information they hold about individuals.

The key question that participants asked themselves when considering justifiability was:

? *Can the service demonstrate that they had considered the potential impacts, done whatever they could to mitigate negative consequences, and*

ultimately determined that the benefits – to service providers, individuals and/or the wider public – outweighed the potential harm the initiative could cause?

- **That the use of data is defensible.** Are public service bodies able and willing to make a publicly acceptable defence of their decision to use data in a particular way if challenged. These discussions allowed for the fact that while something may be able to be classed as legally, or procedurally, correct there were also ethical, political and normative considerations that impacted upon acceptability. Overall, workshop participants considered that these reservations, while valid, should not be allowed to obstruct opportunities for data sharing that have the potential to deliver substantial benefits to individuals, services and communities. Fundamentally, it was asserted that that public agencies have to ‘*make tough decisions all the time*’ regarding how they deploy their resources, and that the decision of when, how and why to share data was not so very different.

The key questions that participants asked themselves when determining whether a controversial or potentially unpopular use of data was acceptable were:

? *Will this deliver substantial benefits to the public? Are there ways for public service providers to minimise the risks it poses? Are we, as public service providers able, and willing, defend our decision to use data this way in the face of challenges?*



Conclusions following the workshop process

While fully informed consent may be the 'gold standard' for using personal data about individuals, public services already have a wide range of permissions to use data to inform service delivery and planning in ways that do not require this level of public awareness. Making the decision about which of these powers they use, and for what purposes, requires service providers to balance and assess the relative benefits and risks to individuals, and services themselves, in the choices they make about data use.

There are a variety of privacy impact assessment tools and planning frameworks that have been produced to help organisations assess the acceptability of opportunities for data sharing within and between one another. Most of these, however, tend to focus on aspects of the data itself: the identifiability of the data used; the additional precautions necessary when using personally sensitive data; considerations of consent; the reliability of the data; and precautions needed to ensure data security and mitigate risks of misuse or accidental disclosure causing harm. To date, very little focus has been given to supporting organisations to evaluate dimensions of benefit and risk, the types of purposes that they, and the wider public, value most, and the issues that they and the public are most concerned about.

Across all of the workshops it was also stressed that if public confidence and support for increased data sharing for a greater array of purposes is to be translated into the social licence for organisations to use data more widely, then the public also needs to have the opportunity to contribute to the discussions. In order to facilitate this, service providers need to be in a position to more clearly articulate to the public the potential benefits that data use can bring. Without a shared language to talk about public benefits, service providers can find it difficult to articulate any rationale behind the choices they make regarding when, and when not, to make use of the data they hold.

This report, by analysing the criteria workshop participants drew upon to rationalise their choices, attempts to address this gap. By identifying points of common ground among the range of service providers that participated in the workshops, we have been able to identify a number of elements that are seen as necessary for a data sharing initiative to be described as producing 'public benefit':

1. That it enables high quality service delivery which produces better outcomes for people, enhancing their wellbeing;
2. That it delivers positive outcomes for the wider public, not just individuals;
3. That it uses data in ways that respect the individual, and their privacy, not just in the method of sharing, but also in principle;
4. That it both represents and supports the effective use of public resources (money, time, staff) to enable the delivery of what people need/want from public services;
5. That the benefits are tangible, recognised and valued by service providers and the wider public.

6. Moving Forward.... balancing the risks of using data against ambitions to deliver ‘Public Benefit’

This project aimed to establish a greater understanding of how different groups (public sector service providers, the voluntary sector and advocacy groups) make sense of and balance the trade-offs inherent in using and sharing data to improve the provision of public services.

The previous chapters describe how a diverse range of service providers approached this, drawing out common approaches and recurring considerations to provide an overview of how stakeholders from across the public and voluntary sectors tend to assess the potential risks and rewards associated with data sharing.

Our goal, however, is not to simply cast light on the tensions inherent in using personal data in the context of public service delivery. We also want to suggest a way forward by proposing a framework for talking about, and evaluating,

different types of public benefits in ways that acknowledge public concerns regarding how personal data is used alongside service providers’ ambitions to use data more effectively.

These questions are not exhaustive, nor mutually exclusive. Our research, however, suggests that, when addressed collectively, the more answers that fall towards the right-hand side of the scale, the more likely an initiative is to be assessed as acceptable to stakeholders and the wider public, and valued as delivering public benefits.

Framework for Evaluating Public Benefit

The workshop process identified five criteria that need to be considered when determining whether a potential data sharing activity can be described as delivering ‘public benefit’:

1. That it enables high quality service delivery which produces better outcomes for people, enhancing their wellbeing;
2. That it delivers positive outcomes for the wider public, not just individuals;
3. That it uses data in ways that respect the individual, and their privacy, not just in the method of sharing but also in principle;
4. That it both represents and supports the effective use of public resources (money, time, staff) to enable the delivery of what people need/want from public services;
5. That the benefits are tangible, recognised and valued by service providers and the wider public.

The framework on the following pages presents each of the elements alongside a set of evaluation questions that can be applied to a proposed data sharing initiative. The questions have been selected in order to initiate discussions about the various dimensions that data sharing proposals can be measured against, in order to evaluate its potential to deliver ‘public benefit’.³⁹

³⁹ The format of this framework tool has been inspired by the scale presented in the Cabinet Office (2016) Data Science Ethical Framework https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf.

Framework for assessing the merit of a data sharing activity to deliver 'public benefit'

Checklist covering key elements of 'public benefit' Where does your data sharing proposal lie on the scale?

1. That the use of data enables high quality service delivery which produces better outcomes for people, enhancing their wellbeing.	Does the individual's whose data is being used directly benefit from improved service provision?		No direct benefit provided to the individual	Clear and direct benefits provided to the individual
	Is the use of data able to deliver long term, life changing benefits to individuals?		Unlikely to deliver long-term benefits	Very likely to deliver long-term benefits
	Will the use of data have punitive impacts on individuals?		High risk of punitive impacts for individuals	Very low risk of punitive impacts
	What is the risk that individuals or communities will suffer unintended negative consequences as a result of the data sharing i.e. as a result of stigma, discrimination or inappropriate targeting?		High risk of unintended negative consequences	Very low risk of unintended negative consequences
2. That the use of data delivers positive outcomes for the wider public, not just individuals;	Does the use of data deliver wider social benefits?		The benefits are just for individuals	There are multiple types of beneficiaries
	Does the initiative address the root causes of social problems/issues?		The approach addresses the symptoms	It addresses the root cause
	Can the use of data inform strategic service changes in ways that could have significant impacts on both public service providers and community wellbeing in the future?		Limited strategic value to inform service changes	High strategic value to inform service changes

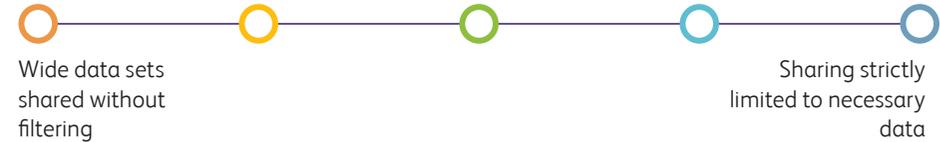
Framework for assessing the merit of a data sharing activity to deliver 'public benefit'

Checklist covering key elements of 'public benefit'

Where does your data sharing proposal lie on the scale?

3. That the initiative uses data in ways that respects the individual, and their privacy, not just in the method of sharing but also in principle.

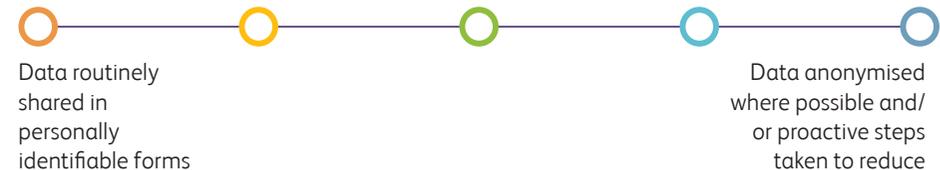
Is only data that is necessary to achieve the purpose being shared?



Wide data sets shared without filtering

Sharing strictly limited to necessary data

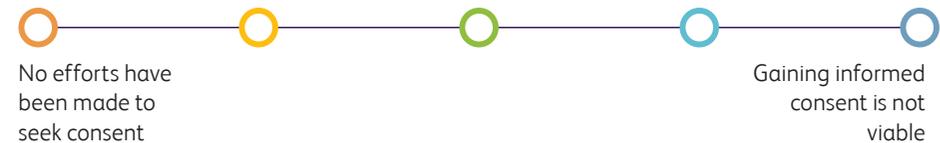
Does the use of data respect the privacy of the individual data subject?



Data routinely shared in personally identifiable forms

Data anonymised where possible and/or proactive steps taken to reduce privacy intrusions

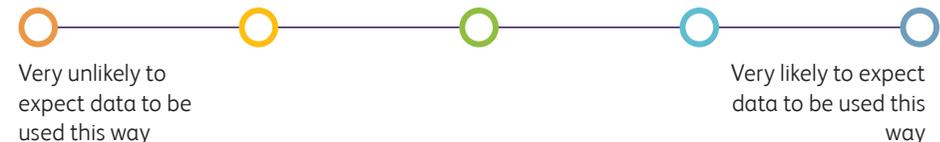
If data is being shared without consent, is it practical to gain informed consent without compromising the value of the data?



No efforts have been made to seek consent

Gaining informed consent is not viable

Could the public reasonably expect data about them to be used for this purpose?



Very unlikely to expect data to be used this way

Very likely to expect data to be used this way

How compatible is this use with the reason the data was originally collected?

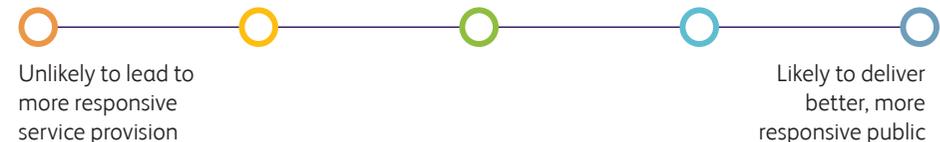


Very incompatible

Very compatible

4. That the use of data both represents, and supports, the effective use of public resources (money, time, staff).

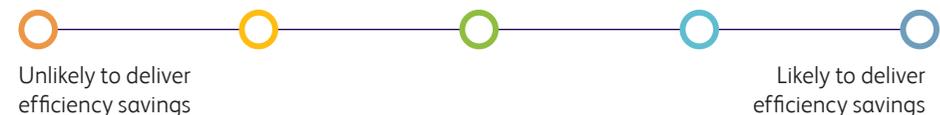
Does the use of data enable the delivery of 'better' public services, able to respond to what the majority of people need/want?



Unlikely to lead to more responsive service provision

Likely to deliver better, more responsive public services

Does the use of data enable strategic planning that will deliver long-term efficiencies?



Unlikely to deliver efficiency savings

Likely to deliver efficiency savings

Framework for assessing the merit of a data sharing activity to deliver 'public benefit'

Checklist covering key elements of 'public benefit' **Where does your data sharing proposal lie on the scale?**

<p>5. That the use of data creates benefits that are visible, recognised and valued by service providers and the wider public.</p>	<p>Are the benefits tangible and measurable?</p>	<p>Benefits are difficult to define</p>	<p>Benefits are tangible and measurable</p>
	<p>Are the benefits delivered able to be clearly attributed to the use of data?</p>	<p>Benefits not directly attributable.</p>	<p>Benefits clearly attributable</p>
	<p>Are the benefits able to be clearly communicated to the public?</p>	<p>Will need considerable explanation to demonstrate value to the public</p>	<p>Benefits will be immediately recognisable to the wider public</p>
	<p>Is the organisation able, and willing, to defend their use of data in this way if objections were raised?</p>	<p>Maybe not.</p>	<p>Absolutely</p>

The proposed use of data may not be recognised as delivering public benefits (but may still be justified on different grounds)

Some issues – think about whether there are ways to move answers further to the right

The proposed use of data is likely to be assessed as delivering 'public benefit'

As already highlighted throughout this report, deciding whether or not a particular use of data is acceptable in the context of public service provision relies on a variety of technical and operational conditions as much as ethical and political factors considered in this framework. This framework is therefore only intended to be used to assess a specific data sharing proposal once an organisation has already established the overall veracity of an initiative: for example, that there is a clear purpose to the data sharing; that there is a legally compliant route for the data to be shared; that the data that is proposed to be used is robust and reliable; the data can be securely stored, used and transmitted; that there are effective oversight and management arrangements in place to protect how the data will be used, and mitigate the risks associated with accidental disclosure or misuse to individuals and service providers; and that the use of data is an efficacious way of achieving the desired outcome (that it is the most efficient and effective use of public resources to address the problem).

How this framework can be used within (and across) organisations

As highlighted previously in this report, service providers do not currently have a clear and consistent set of criteria to use to identify and evaluate the relative public benefits achievable through the better use of data. This framework is designed to help service providers and data controllers (in the first instance) clarify the potential public benefits of data sharing in public service provision, in order to be able to better articulate, and/or justify, the decisions they make about uses of the data they hold.

Internally working through these questions will help service providers clarify and articulate some of the difficult decisions they make regarding how they use data: defining and justifying the trade-offs that they are willing to make regarding the type and sensitivity of data used; the different organisations they include in data sharing arrangements; the incursions into individual privacy and the balance of consent and public awareness they are willing to accept, particularly

in relation to uses that the public may not ostensibly support.

The current disparity in approaches to assessing risk and benefit presents significant challenges, as it can result in a 'patchwork' approach across services and geographies, with little shared knowledge and understanding of best (and worst) practice. Therefore, a more strategic discussion is required, at both local and national levels, and we hope our framework can provide a useful contribution to this.

Involving the public in the discussion

If the social licence for greater data sharing is to be realised to deliver public benefit, then the public also need to have the opportunity to be involved in the discussions. This should not be done simply to generate greater public approval for the use of data. Rather, it should be undertaken in ways that enable the public to help shape the future of data use by engaging in informed and meaningful dialogue with service providers regarding their aspirations for how public services should be provided and their concerns about how data about them should be used.

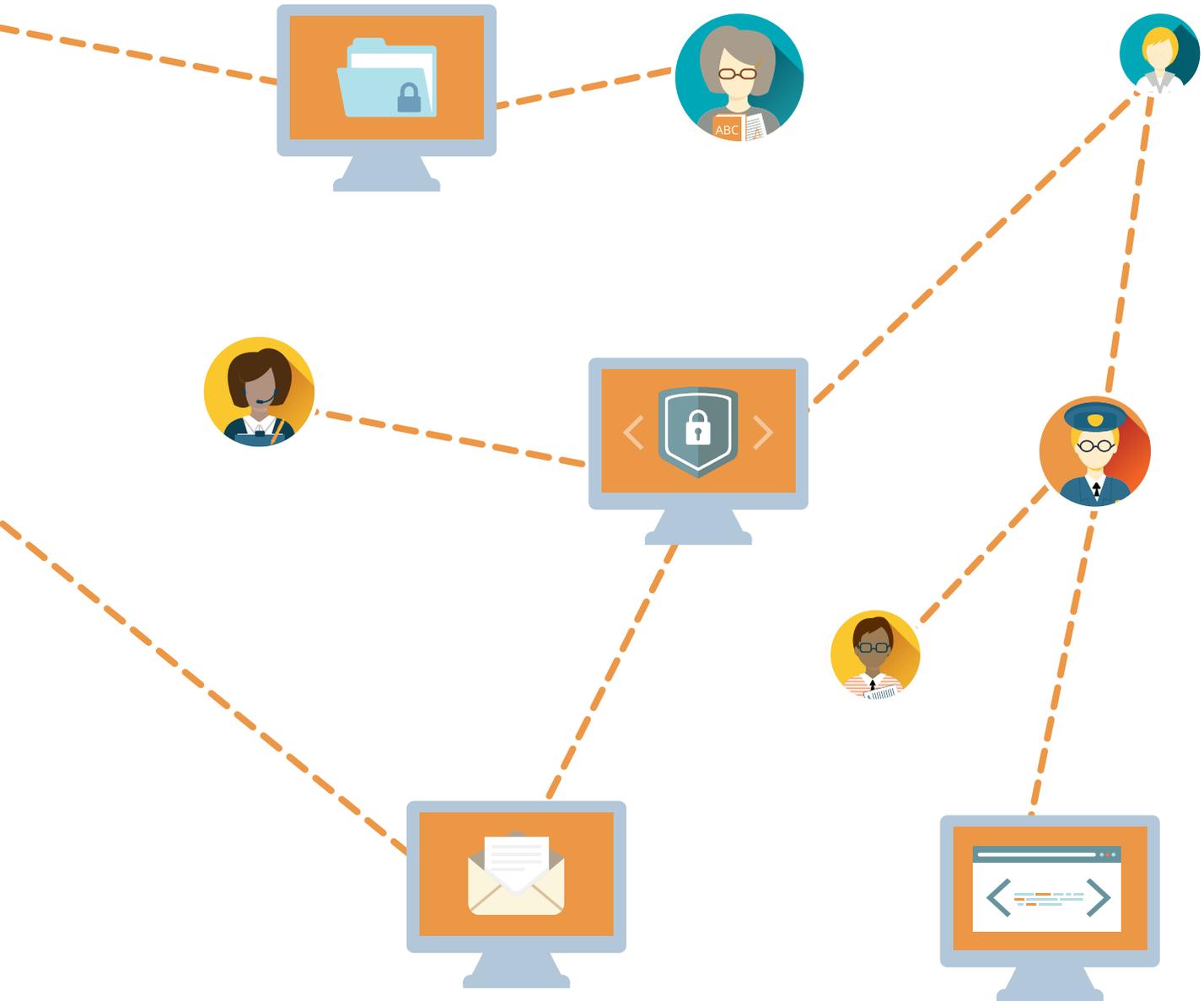
For those organisations and partnerships that want to be at the forefront of data sharing good practice, and who are willing to have the types of difficult conversations that will be required to co-produce acceptable conditions for data use, then a starting point of negotiating a shared understanding of the public benefits people want and expect from data use seems vital.

To enable this, public service providers need to get better at informing the public about how data is currently collected by service providers and the different ways that this information could be used, linked and shared to enhance the delivery of public services. Alongside this, they have a parallel responsibility to raise public awareness about the implications of *not* using the data that is available to its full capacity, and the impacts this could have on how services can be delivered for individuals and for the wider public. Achieving this will involve being able to articulate the underlying tensions

and trade-offs required between using data to deliver benefit and protecting privacy clearly to the public, and the framework provided above can help to do that.

For those organisations that are prepared to invest the time and work with the public, then this framework will also provide a useful tool for initiating conversations with service users, community representatives, and ultimately the wider public, in ways that will increase their understanding of the complexities involved.

While in the short term, the efforts required to begin this process are not insignificant, in the long term, the costs to service providers of not taking the public with them on this journey are likely to be much higher. To not begin these conversations now may undermine the reputation of public service agencies, hamper their ability to resolve disputes, and ultimately constrain their ability to use data in modern, beneficial and potentially transformative ways.



Annex A: Workshop Methodology

In June-July, 2017, staff from [Involve](#) designed and led a series of six workshops in a diverse range of local authority areas across England to explore how professionals from the public and voluntary sectors understand, define and value the public benefits that may be delivered by the better use of data. The purpose was to begin to make sense of where an acceptable balance between risks and benefits may lie for data sharing in the context of public service delivery and to establish a framework for continuing these discussions with both stakeholders and the wider public.

To help focus discussions during the workshops, a [Background Briefing Paper](#) was distributed to attendees in advance. This paper provided:

- Information about the purpose of the workshop and the rationale for the project;
- An outline of the policy drivers for the better use of data to support public service delivery;
- A summary of the legal context for data capture and sharing;
- Definitions of ‘personal data’ and ‘sensitive personal data’ and the protections afforded to each;
- Information about the legal basis for a ‘right to privacy’ and the privacy implications of data sharing;
- An overview of the key areas of tension between data sharing, public benefits and individual privacy.

Workshop Design

The workshops were designed to involve a mixed group of participants, primarily working in small groups (four to six people) in defining, interrogating and evaluating the ‘public benefits’ that could (or could potentially) be achieved by greater data sharing between organisations involved in delivering public services.

In the workshops, a series of examples and case studies were used to prompt discussions⁴⁰. These

⁴⁰ The examples prepared by Involve for use during the workshops can be viewed at <https://www.involve.org.uk/wp-content/uploads/2017/07/workshop-examples.pdf> and the case studies at <https://www.involve.org.uk/wp-content/uploads/2017/07/3-case-studies-data-sharing.pdf>

illustrated how data is being shared and used by public service providers across the country for a variety of purposes, that are all described as delivering ‘public benefit’. Each set of examples was constructed to stimulate debate and discussion (rather than to illustrate good practice) and cut across a range of sectors (housing, health, welfare, social care and community safety). Each involved the use of different types of personal data, shared with different types of organisations, and featured a variety of intended outcomes. As such, the examples were chosen to encourage participants to take a deep-dive into their own understanding of the potential benefits and risks of data sharing. Building in complexity throughout the workshop, the examples challenged participants to develop shared criteria to assess the proportionality, and relative acceptability, of using different types of data for different purposes.

Throughout the workshop series participants also benefited from expert input from:

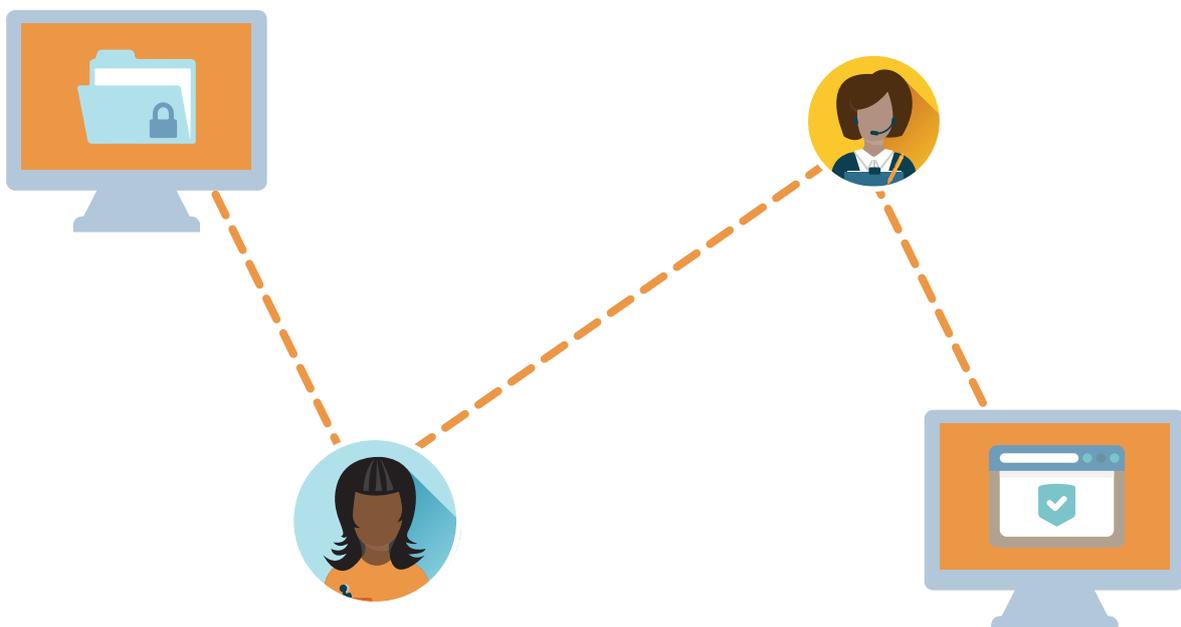
- [Understanding Patient Data’s](#) research into the [best language to use](#) when discussing the different forms in which personal data can be shared, and explaining anonymisation and the likelihood of re-identification;
- Members of the [National Data Guardian’s Panel](#), highlighting how challenges in relation to data sharing, privacy and the public’s expectations of how data about them is used, are being navigated in a health and social care context;
- Staff from the [Open Rights Group](#), discussing how the legislative context for data sharing is changing and the risks and opportunities these changes bring.

These contributors (alongside observers from Carnegie UK Trust and the Centre for Information Sharing Excellence) ‘sat in’ on the discussions at various workshops to provide information and respond to questions, but did not actively participate in the deliberations.

Various exercises were developed for the series of workshops, and not every exercise was used in each location. Instead, the facilitators selected exercises in response to the size of the group, the interests of participants, the local context and the degree to which questions around data sharing were already familiar to participants. The goal was to prompt increasingly in-depth deliberations about the public benefits associated with data sharing. Activities used across the workshop series included:

1. Introducing and framing the conversation
2. Exploring participants initial impressions of the opportunities and challenges associated with data sharing
3. Using examples of data sharing practice to identify dimensions of public benefit: ranking the examples in order of their ability / potential ability to deliver public benefits (negotiating criteria for ranking the examples at each table);
4. Using examples of data sharing practice to identify areas of risk and concern, and then ranking them in order of risk (negotiating criteria for ranking the examples at each table);
5. Expert inputs to help frame the discussions;
6. Working in small groups to 'define' public benefit;
7. Identifying criteria to rank the relative acceptability of different contexts, forms and purposes of data sharing;
8. Using a case study to explore the acceptability of a systematised use of data linking within a local authority area;
9. Using case studies to explore whether the type of personal information shared, the purpose or who it is shared with has the most impact on assessments regarding acceptability; and
10. Plenary discussion focussing on insights, reflections and 'take-aways' from the workshop.

At the conclusion of each workshop a local area report was produced and distributed to participants. These were designed to give local stakeholders a record of the debates and deliberations that took place in their area in order to support participants to continue the discussions they had started with colleagues, partners and local policymakers.



Annex B: Spectrum of Identifiability

These terms were developed by Understanding Patient Data through an extensive engagement process with healthcare workers and the public to determine best language to use when discussing identifiability and anonymisation with a non-expert audience.⁴¹ They found that using pictures is the most helpful way to explain these concepts.

At one end of the spectrum, a person is fully identifiable. As you remove or encrypt information, you blur the image more and more, and it becomes more difficult to identify who that person is. At the other end of the spectrum, it is not possible to identify who someone is — they are effectively anonymous.

Personally identifiable data

This is information that identifies a specific person. Identifiers include: name, address, full postcode, date of birth or NHS number. Personally identifiable information will always be stored in a highly secure way. There are strict laws that safeguard how personally identifiable information can be used if you are not asked for consent. There are also sanctions under the Data Protection Act if personally identifiable data is misused.

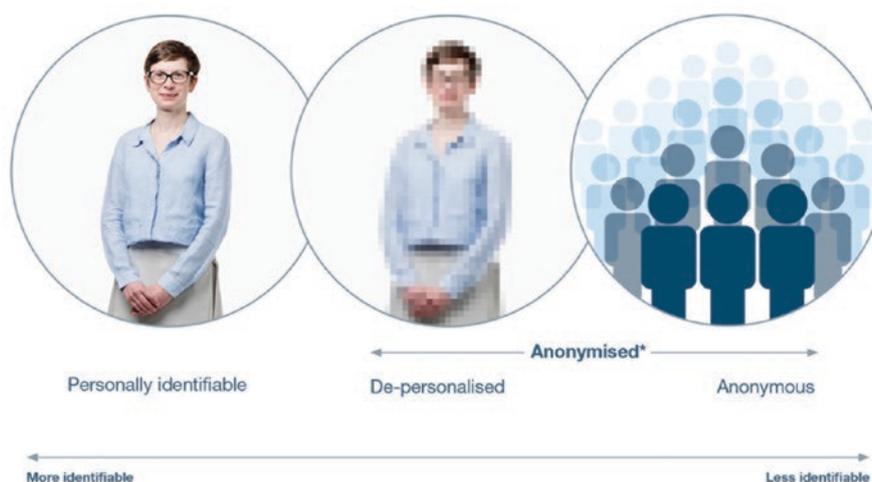
⁴¹ Understanding Patient Data (2017) What are the best words to use when talking about data <https://understandingpatientdata.org.uk/what-are-best-words-use-when-talking-about-data>

Anonymised data

The Information Commissioner's Office gives guidance about what details must be removed or masked, and the safeguards that must be followed to anonymise data effectively. There are two different types of anonymised information: one individual-level, one grouped.

- **De-personalised data** – This is information that does not identify an individual, because identifiers have been removed or encrypted. However, it would, in theory, be possible to reverse that process and re-identify someone, so safeguards are still important. It is just like a blurred photo of someone. We can't immediately see who the person is, but we know it is a specific person. If we had the right computer power, and really needed to know who the person was, it might be possible to work it out. There are strict safeguards on how de-personalised information can be used, because there is the potential that it might be possible to re-identify someone.
- **Anonymous data** – This is information from many people combined together, so that it would not be possible to identify an individual from the data. It may be presented as general trends or statistics. Because it would not be possible to identify someone, this information does not need special protection and can be published openly.

Spectrum of identifiability



Annex C: Legal Context for Data Capture and Sharing

The text below replicates the background information provided to workshop participants about the current legal context for data capture and sharing. It is included here to provide additional background and context for readers less familiar with this field.

A public body may only share data if it has legal authority to do so. The first question that agencies wishing to share data need to ask therefore is whether they have the expressed or implied legal powers to perform a function necessitating data sharing. The power may be set out expressly in statute, or it may be implied from the body's other statutory powers and functions.

Until very recently, the legal power to share data has come from a variety of specific legislative 'gateways' by which information can be disclosed or received for particular purposes. Examples of such permissive statutory gateways include:

- section 115 of the Crime and Disorder Act 1998, allowing anyone to pass information to certain authorities if it is necessary or expedient for the purposes of any provision of the Act;
- section 14 of the Offender Management Act 2007, allowing data sharing between specified bodies for various purposes relating to offenders;
- section 111(1) of the Local Government Act 1972, providing that they 'shall have power to do anything . . . which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions';
- section 6 of the Crime and Disorder Act 1998 which gave police and local authorities the implied power to share data to formulate and implement strategies for reduction of crime in their area; and

- section 25 A, B and C of the Health and Social Care (Safety and Quality) Act 2015 which places a legal duty on health and adult social care organisations to share information when it will facilitate care for an individual.

In May, 2017, the Digital Economy Act was passed by Parliament to enable greater data access for defined public interest purposes by public authorities. Broadly defined, clause 30 of the Digital Economy Act contains provisions for a 'single gateway to enable public authorities, specified by regulation, to share personal information for tightly constrained reasons agreed by parliament, where its purpose is to improve the welfare of the individual in question. To use the gateway, the proposed sharing of information must be for the purpose of one of the specified objectives, which will be set out in regulations.'⁴²

The Digital Economy Act therefore provides new legal mechanisms to allow data sharing between specified public-sector bodies to support the better use of data for targeted interventions; improving the welfare of citizens; reducing debt owed to the public sector; fraud prevention; the sharing of civil registration information; and producing better statistics and research. These powers are to be regulated by codes of practice that have yet to be published.

Health data, however, is considered particularly sensitive and there are additional restrictions and conditions on its sharing, including the common law duty of confidentiality. The Digital Economy Act, for example, explicitly excludes the use of health data from its permissions for research purposes and health services are not currently included in the list of specified public bodies. The 2013 Caldicott Review of Information Governance established four legal bases for processing personal confidential health and social

42 UK Government (2017) Digital Economy Act <http://www.legislation.gov.uk/ukpga/2017/30/part/5/enacted> (accessed 28/5/2017)

care information which meet the common law duty of confidentiality. These are: with consent, through statute, through a court order and ‘when the processing can be shown to meet the “public interest test”, meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.’⁴³

Once it has been established that the parties have the necessary powers to share data, the next step is to consider whether the proposed sharing is compatible with other legal provisions regulating the use of personal data. For example, data sharing by public authorities must also comply with the European Convention of Human Rights (now part of the UK domestic law as a result of the Human Rights Act 1998), and in particular Article 8, which provides: Everyone

has the right to respect for his private and family life, his home and his correspondence⁴⁴. It also must comply with the requirements of the Data Protection Act 1998 (DPA).⁴⁵

From May, 2018, the General Data Protection Regulation (GDPR)⁴⁶ will apply in the UK, and the Government has confirmed that leaving the EU will not affect the commencement of the GDPR.⁴⁷ The GDPR will replace the Data Protection Directive 95/46/ec as the primary law regulating how personal data is protected and is intended to harmonise data privacy laws across Europe, to protect and empower all EU citizens’ data privacy and to reshape the way organisations across the region approach data privacy.

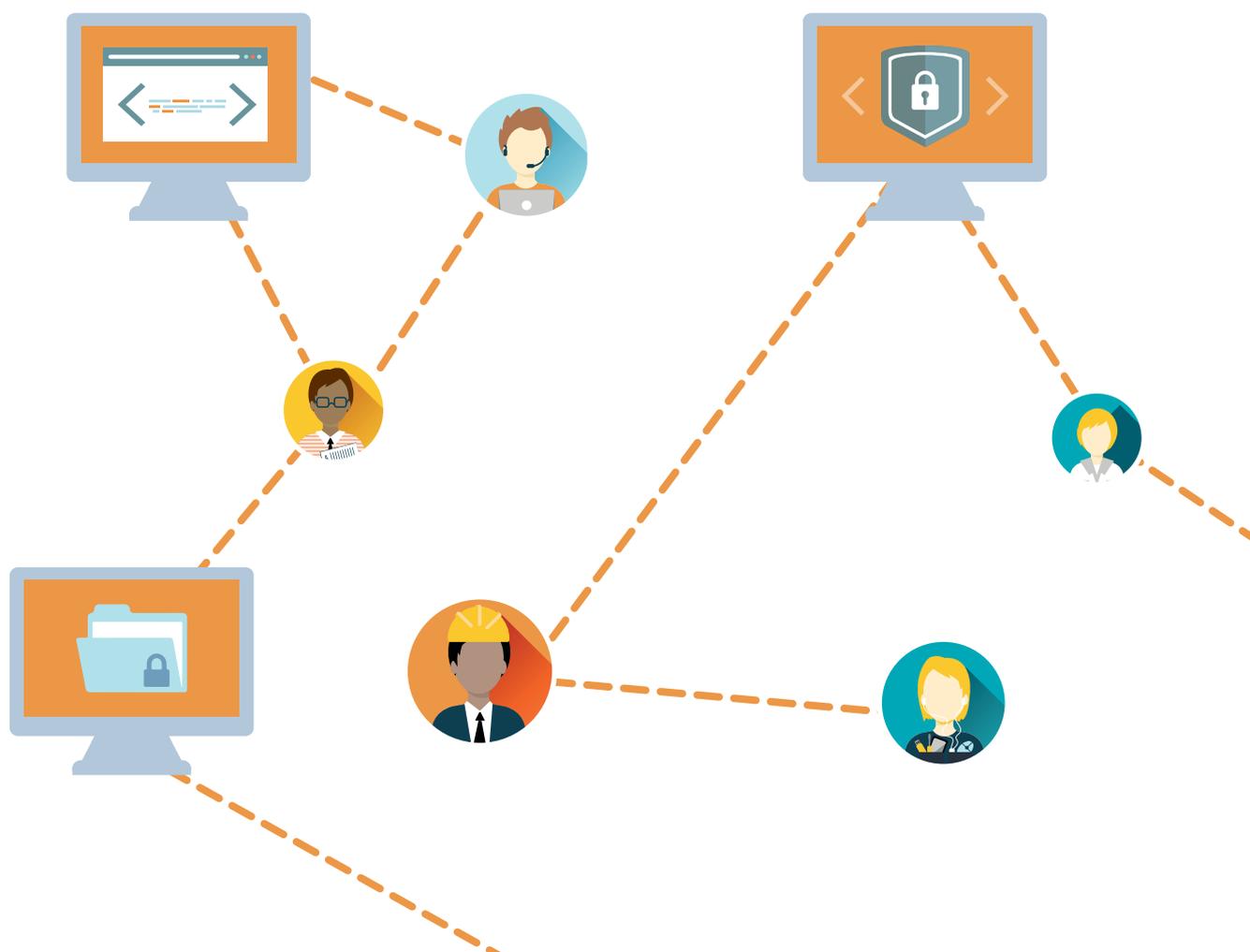
43 National Data Guardian (2013) Information: To Share Or Not To Share? The Information Governance Review https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

44 UK Government, (1998) Human Rights Act https://www.legislation.gov.uk/ukpga/1998/42/pdfs/ukpga_19980042_en.pdf

45 UK Government (1998) Data Protection Act <https://www.legislation.gov.uk/ukpga/1998/29/contents> (accessed 28/5/2017)

46 European Union (2016) General Data Protection Regulation <https://gdpr-info.eu/> (accessed 4/12/2017)

47 Information Commissioner’s Office (2017) Overview of the General Data Protection Regulation (GDPR) <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>



Annex D: Defining Personal Data

The Data Protection Act (1998) defines personal data as being ‘data which relate to a living individual who can be identified from those data, or from those data and other information which are in the possession of, or are likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.’⁴⁸

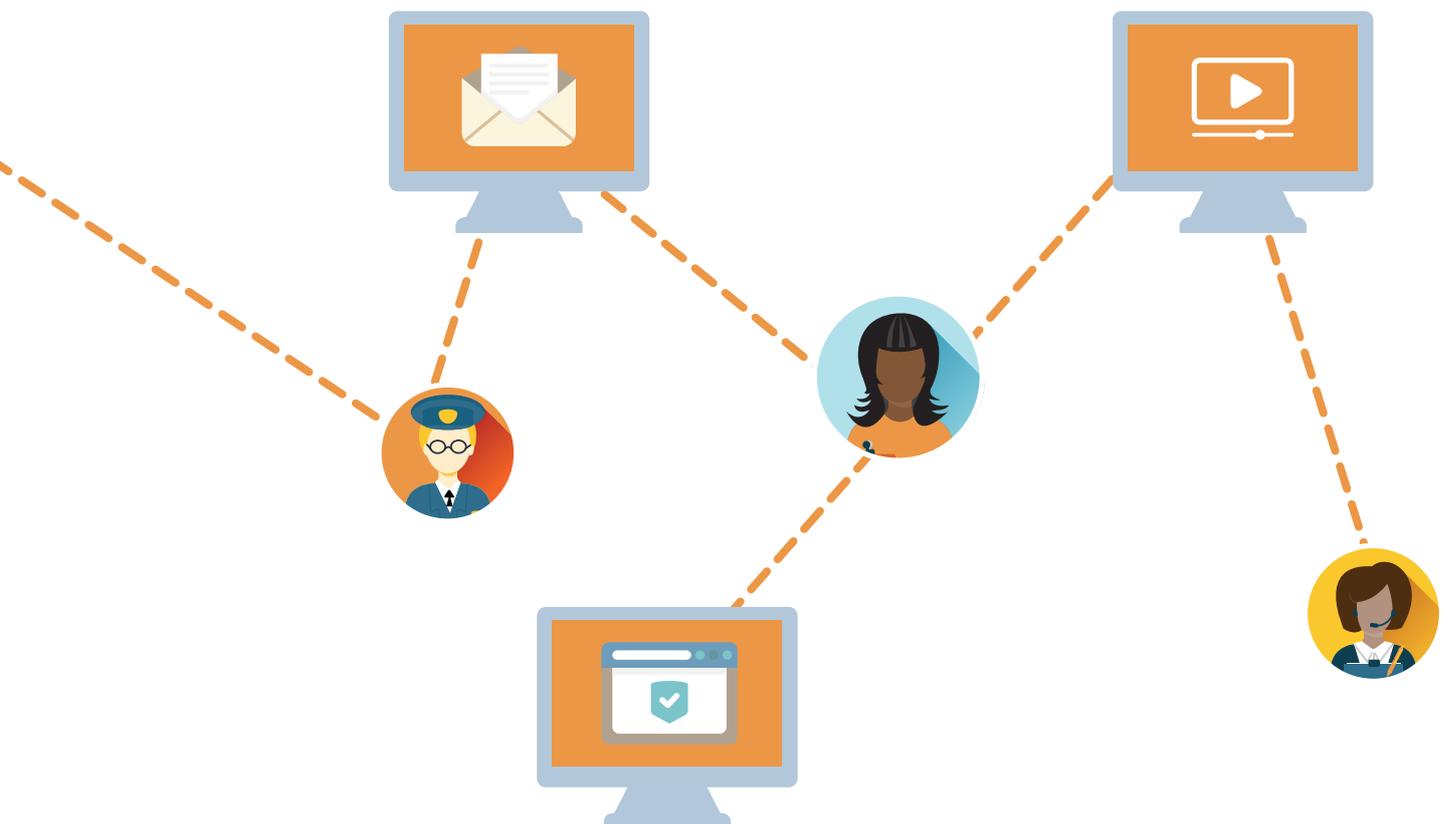
The Act further notes that there are some forms of personal data that are likely to be of a private nature are additionally sensitive because information about these matters could be used in a discriminatory way. Sensitive personal data is taken to include information related to racial or

ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexuality and criminal justice history, and needs to be treated with greater care than other personal data. There are also **additional protections** included within the Act to ensure that sensitive personal data is processed and stored securely and its use is controlled.

The General Data Protection Regulation, which comes into force in May 2018, provides a more detailed and expansive definition of personal data and makes it clear that information such as online identifiers – such as an IP address – can be personal data⁴⁹, reflecting changes in technology and the way organisations collect information about people.

48 UK Government (1998) Data Protection Act <https://www.legislation.gov.uk/ukpga/1998/29/contents> (accessed 28/5/2017)

49 European Union (2016) General Data Protection Regulation <https://gdpr-info.eu/> (accessed 4/12/2017)



Annex E: The Right to Privacy

Privacy is a qualified, fundamental human right. The right to privacy is articulated in all of the major international and regional human rights instruments, including the United Nations Declaration of Human Rights (UDHR) 1948, Article 12 which states:

‘No-one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’⁵⁰

Individual privacy is, in the context of data sharing debates, fundamentally the ability of individuals to choose when they wish to disclose personal information about themselves, and who they want to disclose this information to. Individual privacy, therefore, can be threatened or breached through a number of practices associated with data sharing, each of which has the ability to produce a different form of harm. The list below, adapted from Solove’s *A Taxonomy of Privacy*⁵¹ itemises the types of harm that different aspects of the process and outcomes of data sharing can have on individual privacy:

Information processing

- Aggregation – The combination of various pieces of data about a person
- Identification – Linking information to particular individuals
- Insecurity – Carelessness in protecting stored information from leaks and improper access
- Secondary use – Use of information collected for one purpose for a different purpose without the data subject’s consent
- Exclusion – Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data

Information dissemination

- Breach of confidentiality – Breaking a promise to keep a person’s information confidential
- Disclosure – Revelation of information about a person that impacts the way others judge her character
- Increased accessibility – Amplifying the accessibility of information
- Distortion – Dissemination of false or misleading information about individuals

Invasion

- Intrusion – Invasive acts that disturb one’s tranquillity or solitude
- Decisional interference – Incursion into the data subject’s decisions regarding her private affairs

Further, unlike most other rights, an individual’s privacy can be compromised without them necessarily being aware that it is taking place: ‘With other rights, you are aware of the interference – being detained, censored, or restrained. With other rights, you are also aware of the transgressor – the detaining official, the censor, or the police.’⁵²

The Data Protection Act gives individuals certain specific rights over their personal data. These include:

- the right to access personal data held about them;
- the right to know how their data is being used; and
- the right to object to the way their data is being used.

50 United Nations (1948) Declaration of Human Rights <http://www.un.org/en/universal-declaration-human-rights/> (accessed 28/5/2017)

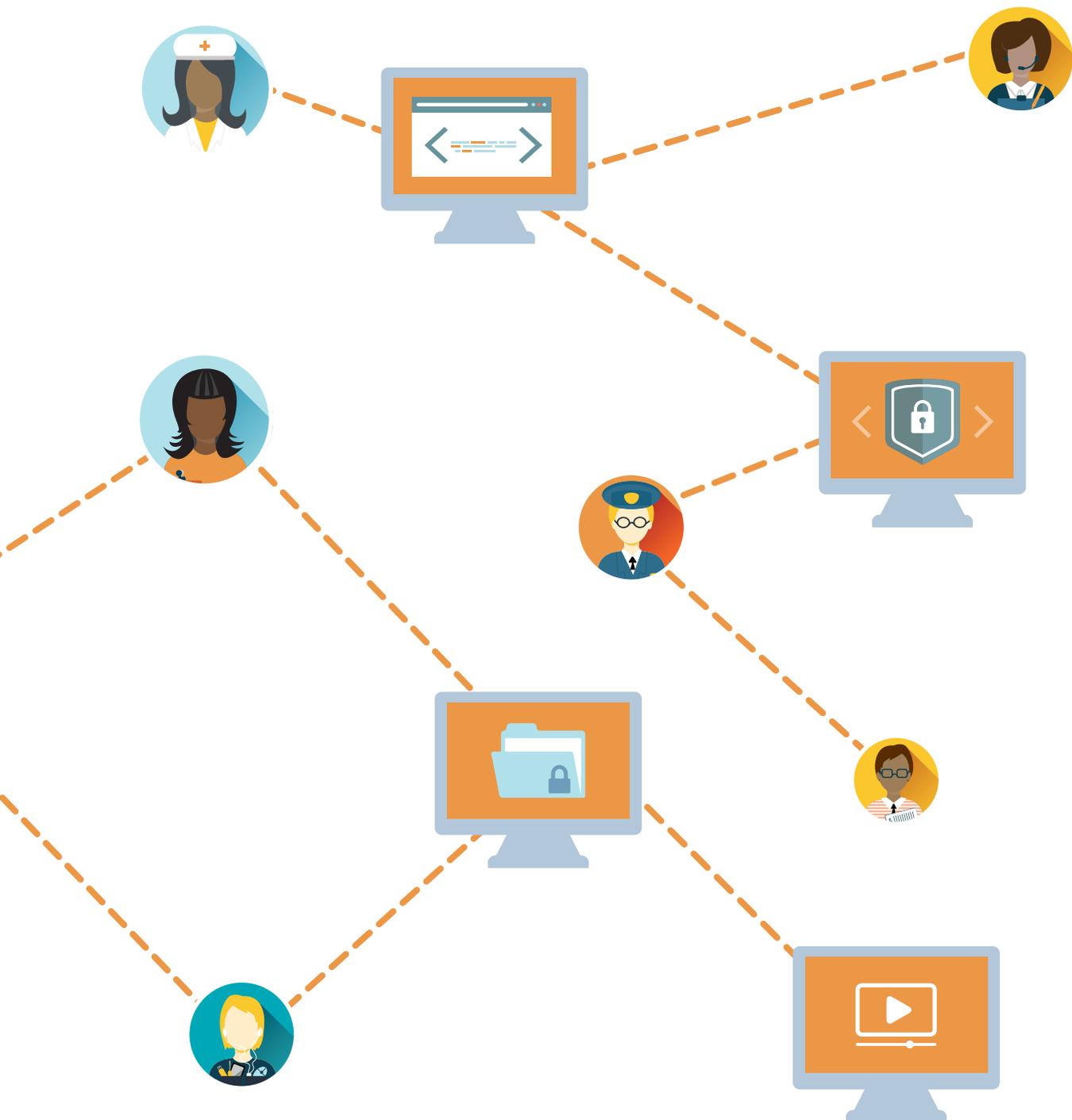
51 Solove, D.J. (2006) *A Taxonomy of Privacy*. University of Pennsylvania Law Review 154(3): 477-560.

52 Privacy International (2017) What is Privacy? <https://www.privacyinternational.org/node/54> (accessed 28/5/2017)

Individuals can object when the use of their personal data is causing them ‘substantial, unwarranted damage or substantial, unwarranted distress’. The objection can be to a particular use of information or to the fact an organisation is holding their personal data at all. Organisations are required by law to respond to individuals who object in writing to the way their personal

data is being used. ‘However, they do not need to comply with the request unless there is damage or distress and this is substantial and unwarranted.’⁵³

53 Information Commissioner’s Office (2011) Data Sharing Code of Practice. https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf



For more information

Carnegie UK Trust

Andrew Carnegie House
Pittencrieff Street
Dunfermline
KY12 8AW

Tel: +44 (0)1383 721445
Email: info@carnegieuk.org
www.carnegieuktrust.org.uk

Involve

18 Victoria Park Square
London
E2 9PF

Tel: +44 (0) 20 3745 4334
Email: info@involve.org.uk
www.Involve.org.uk

Understanding Patient Data

215 Euston Road
London
NW1 2BE

Tel: +44 (0)20 7611 5765
Email: hello@understandingpatientdata.org.uk
www.understandingpatientdata.org.uk

Lead Author: Kaela Scott

Contributors: Simon Burall, Nicola Perrin, Philippa Shelton, Douglas White, Gail Irvine and Anna Grant.

April 2018



CHANGING MINDS • CHANGING LIVES

Carnegie United Kingdom Trust
Registered charity SC 012799 operating in the UK
Registered charity 20142957 operating in Ireland
Incorporated by Royal Charter 1917

ISBN 978-1909447820

