REFORM

Sharing the benefits
How to use data effectively in the public sector

Sarah Timmis
Luke Heselwood
Eleonora Harwich

#reformdatasharing

Sharing the benefits

How to use data effectively in the public sector

Sarah Timmis
Luke Heselwood
Eleonora Harwich

Acknowledgements

Reform

Reform is an independent, non-party think tank whose mission is to set out a better way to deliver public services and economic prosperity. Our aim is to produce research of outstanding quality on the core issues of the economy, health, education, welfare, and criminal justice, and on the right balance between government and the individual.

Reform is a registered charity, the Reform Research Trust, charity no.1103739. This publication is the property of the Reform Research Trust.

---

1   See Appendix for further details.

Contents

Executive summary

This report demonstrates the potential of data sharing to transform the delivery of public services and improve outcomes for citizens. It explores how government can overcome various challenges to 'get data right' and enable better use of personal data within and between public-sector organisations.

Ambition meets reality

Government is set on using data more effectively to help deliver better public services. Better use of data can improve the design, efficiency and outcomes of services. For example, sharing data digitally between GPs and hospitals can enable early identification of patients most at risk of hospital admission, which has reduced admissions by up to 30 per cent in Somerset. Bristol's Homeless Health Service allows access to medical, psychiatric, social and prison data, helping to provide a clearer picture of the complex issues facing the city's homeless population. However, government has not yet created a clear data infrastructure, which would allow data to be shared across multiple public services, meaning efforts on the ground have not always delivered results.

The data: sticking points

Several technical challenges must be overcome to create the right data infrastructure. Individual pieces of data must be presented in standard formats to enable sharing within and across services. Data quality can be improved at the point of data collection, through better monitoring of data quality and standards within public-sector organisations and through data-curation-processes.

Personal data also needs to be presented in a given format so linking data is possible in certain instances to identify individuals. Interoperability issues and legacy systems act as significant barriers to data linking. The London Metropolitan Police alone use 750 different systems, many of which are incompatible. Technical solutions, such as Application Programming Interfaces (APIs) can be overlaid on top of legacy systems to improve interoperability and enable data sharing. However, this is only possible with the right standards and a solid new data model. To encourage competition and improve interoperability in the longer term, procurement rules should make interoperability a prerequisite for competing companies, allowing customers to integrate their choices of the most appropriate products from different vendors.

Building trustworthiness

The ability to share data at scale through the internet has brought new threats to the security and privacy of personal information that amplifies the need for trust between government and citizens and across government departments. Currently, just 9 per cent of people feel that the Government has their best interests at heart when data sharing, and only 15 per cent are confident that government organisations would deal well with a cyber-attack. Considering attitudes towards data sharing are time and context dependent, better engagement with citizens and clearer explanations of when and why data is used can help build confidence. Auditability is also key to help people and organisations track how data is used to ensure every interaction with personal data is auditable, transparent and secure.

Legal complexities

The legal framework around data sharing is often described as highly complex. New legislation, such as the General Data Protection Regulation (GDPR), sits on top of pre-existing frameworks, which can create a nebulous system for public-sector organisations to navigate. Every time information is shared, public-sector organisations must go through the process of creating or finding the right legal 'gateway' to enable sharing in a secure way, which can take years. Legislation has at times struggled to keep pace with the rapidly evolving way in which data is being used. It is, therefore, crucial to provide mediums which demystify legislation for those trying to understand how to use data properly within the legal landscape.

The enablers

Creating a new data infrastructure which allows organisations to overcome barriers to data sharing and build on government promises outlined in its *Transformation Strategy*, requires clear leadership and a collaborative approach. Opportunities are arising to redirect leadership through new structures, such as the Data Advisory Board, and new positions, such as the Chief Data Officer. Local government can also play an important role in promoting data sharing across the public sector. Local data-sharing agreements can provide an infrastructural and standards template for larger-scale data-sharing agreements. Building on these models can help spread best practice and improve data-sharing standards across the country.

Recommendations

1. Public-sector organisations should offer synthetic datasets, which they can share with others so that requests for data adhere to the right data standards in each organisation.

2. Within the Government's Framework for Data Processing, the Department for Digital, Culture, Media and Sport should create a Data Quality Assurance Toolkit and ensure that public-sector bodies submit data to be tested.

3. The Department for Digital, Culture Media and Sport should create a seal of approval, similar to the O'Neil Risk Consulting & Algorithmic Auditing (ORCAA), which indicates that data quality is satisfactory and that biases within datasets have been accounted for.

4. Technology vendors selling to public-sector bodies should ensure that their products are compatible with relevant Application Programming Interfaces (APIs), allowing this technology to overcome interoperability issues and government to change providers with ease.

5. Moving forward, it should be mandatory for any system procured within the public sector to adopt open standards, encouraging competition and improving interoperability by avoiding vendor lock-in situations.

6. Government departments should identify and support initiatives like Understanding Patient Data in all policy areas, supporting organisations if they need to properly engage citizens and understand how they want their data to be used across public services.

7. All government departments should prepare to develop audit trails which track how data is used to ensure every interaction with personal data is auditable, transparent and secure.

8. Government should, in partnership with the Information Commissioner's Office, investigate and publicise the optimum training needed to familiarise public servants with the handling of personal data, to reduce the fear of using and sharing personal data.

9. The Information Commissioner's Office should continue to partner with specialist organisations, like the former Centre of Excellence for Information Sharing, who help demystify legislation, with resources and case studies specifically catered to public-sector bodies.

10. The new Data Advisory Board should focus its attention on tackling the difficult challenges stopping effective multi-agency data sharing. The Advisory Board should include a representative from each department to ensure collective responsibility.

11. Data-sharing policy should be included in the remit of the Chief Data Officer, so there is a specific individual championing best practice towards data sharing across siloed departments.

12. Leadership on the sharing of individuals' personal data should come from the Cabinet Office rather than the Department for Digital, Culture, Media and Sport to help to ensure that the Government's data-sharing strategy has influence that reaches across departments.

13. Local government should play an important role in the establishment of data standards and infrastructure. By giving local areas space to try and test data-sharing arrangements, it will help to demonstrate which projects are successful and could be scaled-up regionally and nationally.

Introduction

Government sits at the heart of a web of data on individuals. Every time someone visits their GP, pays taxes, or sits an exam, data is collected. This data is recorded, analysed, and sometimes shared to allow services to better understand user needs and best "fulfil their functions".[2] Without proper access to this data, there can be gaps in service provision which can lead to poor outcomes.[3] Being able to share data at scale has been made possible by the advent of the internet and the World Wide Web.[4] However, this has raised issues around security, privacy and consent. A solid infrastructure for sharing personal data[5] in the public sector is therefore critical.

Successive governments have made the provision of joined-up, citizen-centred services underpinned by data sharing the focus of their public service reform agenda.[6] The "effective data use in government" by the public sector is still an integral part of the current Government's *Transformation Strategy*.[7] Nevertheless, the Government's efforts to 'get data right' have not yet lived up to its ambition. Its reports have not been explicit enough on how to create a distributed and governable data infrastructure that would enable the delivery of these plans. This lack of clarity has led to a patchy realisation of benefits on the ground.

The Government has focused much of its efforts on easier "quick wins", such as open data, according to interviewees for this paper. Open data is less sensitive than an individual's personal data and therefore much easier to deal with. However, pockets of best practice can be found around the country, where data has been successfully accessed and used across public-sector organisations for a specific purpose and led the public benefit.[8]

This paper sets out to examine how personal data could be better accessed and used within and between public-sector organisations to improve the delivery of services for citizens and ultimately improve outcomes.[9]

---

2   Dean Machin, *Data and Public Policy – Trying to Make Social Progress Blindfolded,* Information Commissioner's Office, 2015, 5.

3   National Audit Office, *Transforming Rehabilitation*, 2016; HM Inspectorate of Probation, *Transforming Rehabilitation: An Independent Inspection of the Arrangements for Offender Supervision*, 2016; Peter Sidebotham et al., *Pathways to Harm, Pathways to Protection: A Triennial Analysis of Serious Case Reviews 2011 to 2014* (Department for Education, 2016); Dr Androulla Johnstone, *Independent Investigation into the Care and Treatment Provided to Mr X, Ms Y and Mr Z by the Dorset HealthCare University NHS Foundation Trust* (Health and Social Care Advisory Service, 2015); Bob Green et al., *Independent Review of Deaths of People with a Learning Disability or Mental Health Problem in Contact with Southern Health NHS Foundation Trust April 2011 to March 2015* (Mazars, 2015).

4   Thomas Hardjono, *Trust :: Data, A New Framework for Identity and Data Sharing* (Visionnary Future, 2016).

5   See Glossary for definitions.

6   Colin Combe, 'Observations on the UK Transformational Government Strategy Relative to Citizen Data Sharing and Privacy', *Transforming Government: People, Process and Policy* 3, no. 4 (October 2009): 395; Perri 6, Christine Bellamy, and Charles Raab, 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management', *Policy & Politics* 38, no. 3 (July 2010): 465; Cabinet Office, *Government Transformation Strategy*, 2017.

7   Cabinet Office, *Government Transformation Strategy*, 10.

8   Cheryl Davenport, *Integrating Care and Health Information across Leicester, Leicestershire and Rutland*, 2015; Social Finance, *New Insights into Improving Outcomes for At-Risk Youth*, 2016; Social Finance, *Commissioning for Outcomes across Children's Services and Health and Social Care*, 2015.

9   The authors acknowledge that public-sector data can be shared for many other purposes than that of direct service delivery or service design, such as for research purposes. However, to narrow the scope of this paper these other types of data sharing will not be addressed.

1
Ambition meets reality

Across the public sector, large amounts of data about people's interaction with public services are collected every day.[10] The Government has clearly expressed its ambition to harness this data to deliver better services.[11] However, there is a discrepancy between its ambition and the reality on the ground. This discrepancy can be explained by a lack of focus on the question of how to build a secure data infrastructure necessary to deliver the vision of joined-up public services.

1.1   Why share data?

Successive governments have expressed the desire to transform public-service provision by using data to create joined-up services centred around people's needs.[12] The 2005 *Transformational Government* white paper "emphasised the critical link between more vigorous exploitation of personal information and the Government's ambitions for social justice, 'citizen-centric' government and 'personalised' services".[13] This ambition was further reinforced by some high-profile cases highlighting the dramatic costs of not sharing information, such as the case of baby P.[14]

The current Government has had similar aims to harness data effectively in the public sector.[15] In 2016, it published a consultation on the *Better Use of Data in Government*.[16] This formed the basis of the data-sharing principles found in the *Digital Economy Act,* which meant to facilitate the creation of data-sharing gateways[17] between public bodies "where there is a clear public need and benefit".[18]

Sharing data can have a significant impact on the design and efficiency of public services as well as the outcomes they deliver. Social issues are generally complex, multifaceted and have an impact on one another.[19] Understanding individual needs within this landscape can be complex. Used wisely, data can help government understand and design services to fit the population's needs and therefore fulfil its aim of creating joined-up and personalised public services.[20] Figure 1 illustrates how the better use of personal data across different public-sector organisations can improve a person's experience of the service and deliver better outcomes.

10   Rob Wilson et al., 'New Development: Information for Localism? Policy Sense-Making for Local Governance', *Public Money & Management* 31, no. 4 (May 2011): 295.
11   Cabinet Office, *Government Transformation Strategy*; John Manzoni, 'Big Data in Government: The Challenges and Opportunities', Speech, 21 February 2017.
12   Perri 6, Bellamy, and Raab, 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management'; Cabinet Office, *Transformational Government: Enabled by Technology*, 2005; Cabinet Office, *Government Transformation Strategy*; Sarah Gold, 'Data Sharing in the Government Transformation Strategy', IF, 15 February 2017; Mike Bracken, 'Government as a Platform: The next Phase of Digital Transformation', *Government Digital Service*, 29 March 2015.
13   Perri 6, Bellamy, and Raab, 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management', 465.
14   Local Safeguarding Children Board, *Serious Review Case: Baby Peter*, 2009; Perri 6, Bellamy, and Raab, 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management', 466.
15   HM Revenue and Customs, *Sharing and Publishing Data for Public Benefit*, 2013; Cabinet Office, *Government Transformation Strategy*; HM Government, *Digital Economy Act 2017*; Department for Digital, Culture, Media & Sport, *UK Digital Strategy 2017*, 2017; John Manzoni, 'Big Data in Government: The Challenges and Opportunities'; Professor Sir John Bell, *Life Sciences Industrial Strategy – A Report to the Government from the Life Sciences Sector* (HM Government, 2017).
16   Cabinet Office and Government Digital Service, *Better Use of Data in Government*, 2016.
17   See glossary for definition.
18   HM Government, *Digital Economy Act 2017*.
19   Alex Bate, *The Troubled Families Programme (England)*, CBP 07585 (House of Commons Library, 2016); Rachel Pugh, 'The GP Practice Sharing Data to Transform Care for Homeless People', *The Guardian*, 22 February 2017; Ministry of Justice, *Transforming Rehabilitation: A Strategy for Reform*, 2013.
20   Cabinet Office, *Modernising Government* (London: Stationary Office, 1999); Patrick Dunleavy, 'The Future of Joined-up Public Services 2020', 2010, 34; NHS England, *Five Year Forward View*, 2014; National Audit Office, *Personalised Commissioning in Adult Social Care*, 2016.

Figure 1: Troubled Families in Staffordshire

The sharing of personal data can help meet the Government's aims of reducing fragmentation between public bodies and designing services tailored to the individual. In Staffordshire, the 'Building Resilient Families and Communities' (BRFC) project – the local vision for its Troubled Families Programme – uses personal data across services to improve their design. The programme identified mental-health problems as a key issue facing the local area[21] and as a result, the BRFC signed an Information Sharing Agreement with South Staffordshire and Shropshire Healthcare NHS Foundation Trust to provide a legal basis for the sharing of mental-health data. This agreement has enabled the BRFC to direct resources more effectively and provide mental-health training for frontline BRFC workers and a new relationship with the local Mental Health Trust to improve referrals.[22]

As highlighted by the Information Commissioner's Office (ICO), data sharing can occur systematically when the "same data sets are shared between the same [or different] organisations for an established purpose"[23] or when there is a statutory obligation to do so. Figure 2 highlights some of the ways in which data sharing can be defined and the definition used in this paper.

Figure 2: What does data sharing mean?

Data sharing can be broadly understood as 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."[24]

It can be defined as a transactional relationship between:

> The individual who is the subject of personal data – the data subject;

> The "person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed"[25] – the data controller – and;

> Any "person, other than an employee of the data controller, who processes the data on behalf of the data controller"[26] – the data processor.

The rights and obligations of the parties involved in a data-sharing agreement are enshrined the General Data Protection Regulation (GDPR) which came into effect in May 2018, replacing the 1998 Data Protection Act.[27] The specific purpose of sharing data within and between public-sector bodies can vary.[28]

Data sharing is often understood as the transfer of data from one organisation to another with the data physically moving from one organisation to another. However, this is not the definition used in this paper as there is no need for the data to physically move from one place to another.[29] What matters is that organisations can access data held by other organisations without the need for transferring data.[30]

---

21 Centre of Excellence for Information Sharing, 'How Information Sharing Is Improving Help for Troubled Families', Webpage, 2018.
22 Centre of Excellence for Information Sharing, *Sharing Health Data to Improve Outcomes for Families and Children: Staffordshire Case Study*, 2016, 11–14.
23 Information Commissioner's Office, *Data Sharing Code of Practice*, 2011, 9.
24 Ibid.
25 Information Commissioner's Office, *Guide to Data Protection*, 2017.
26 Ibid.
27 Information Commissioner's Office, 'Guide to Data Protection', Webpage, 1 June 2018.
28 Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, 2018.
29 Alex Pentland et al., 'Towards the Internet of Trusted Data', in Trust: *Data, A New Framework for Identity and Data Sharing*, ed. Thomas Hardjono, David Shrier, and Alex Pentland (Visionary Future, 2016), 45–49.
30 Ibid.

1.2   The reality

The public sector has not lived up to its ambition of creating joined-up public services underpinned by an effective system for sharing data across multiple organisations.[31] Efforts on the ground have not always delivered results and have often focused on a given policy area. Nevertheless, pockets of best practice do still exist as highlighted by Figure 3 and Figure 4.

Figure 3: Risk stratification in Somerset

Accessing and linking data together are the stepping stones for understanding population needs,[32] stratifying individuals by risk,[33] and supporting personalised care.[34] It can help health professionals identify patients with distinctive needs, define types of care for different patient groups, prioritise more vulnerable patients, monitor outcomes and budget effectively.[35] In Somerset, data from GPs, hospital activity and health conditions are collected and linked to help healthcare practitioners identify patients most at risk of hospital admission.[36] It allows clinicians to focus services on this high-risk group. This risk stratification tool, which was piloted in 2009, is now used by 98 per cent of GPs in Somerset to identify high-risk patients.[37] The pilot has helped to reduce hospital admissions by 30 per cent in Somerset.[38]

Figure 4: Tackling homelessness in Bristol

Bristol's Homeless Health Service allows access to medical, psychiatric, social and prison data, helping to provide a clearer picture of the complex issues facing the city's homeless population.[39]
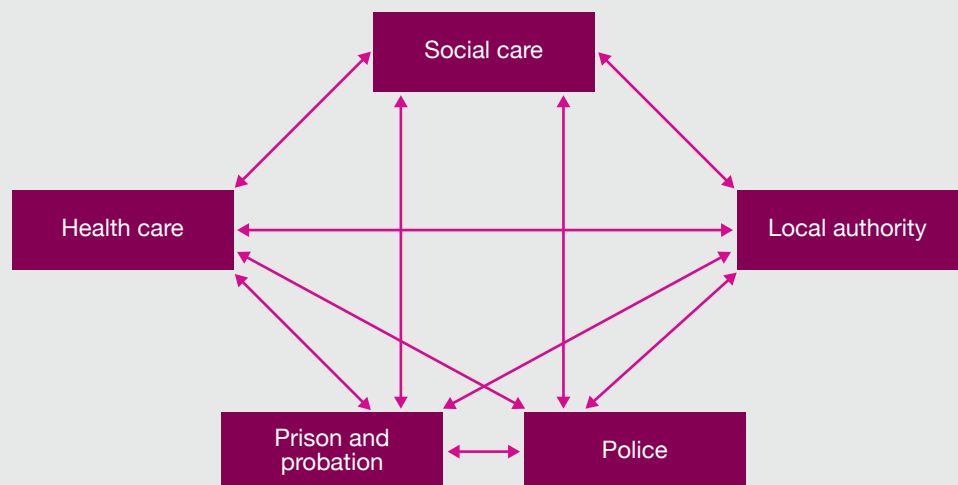
31   Rob Wilson et al., 'New Development: Information for Localism? Policy Sense-Making for Local Governance', 295.
32   Department of Health et al., "Section 1: Population Segmentation, Risk Stratification and Information Governance," in *How to Guide: The BCF Technical Toolkit*, ed. The Better Fund, 2014, 2.
33   Ibid.; Martin Roland and Gary Abel, 'Reducing Emergency Admissions: Are We on the Right Track?', British Medical Journal 345 (18 September 2012).
34   NHS England, *Using Case Finding and Risk Stratification: A Key Service Component for Personalised Care and Support Planning*, 2015, 5.
35   Department of Health et al., "Section 1: Population Segmentation, Risk Stratification and Information Governance," 2-3. NHS England, *Using Case Finding and Risk Stratification: A Key Service Component for Personalised Care and Support Planning*, 10.
36   NHS South, Central and West, 'Risk Stratification Tools in Somerset • South, Central and West CSU', Webpage, 2018.
37   Ibid.
38   Ibid.
39   Rachel Pugh, 'The GP Practice Sharing Data to Transform Care for Homeless People'.

By providing a fuller picture of a person's circumstances, the Homeless Health Service helps to triage people to the correct service. For example, police attending a drunk and disorderly individual can access a data platform to see if they are known to local mental health teams – meaning that they can be referred to this team, rather than "unnecessary sectioning or a night in police cells".[40] In 2017, over 450 records were viewed by health professionals to provide more efficient joined-up care.[41] The same year, the Care Quality Commission awarded the service an "Outstanding" rating, stating that the sharing of information ensured a "holistic assessment" of patients.[42]

Figure 3 and Figure 4 highlight the existence of pockets of best practice across various public-sector organisations. However, not all programmes are as successful. The Ministry of Justice's (MoJ) *Transforming Rehabilitation Strategy* provides an example of a programme that has not managed to create an infrastructure to appropriately share data between various organisations.[43] Community Rehabilitation Companies, who provide probation services, are not always informed whether a person who is released from prison has suffered from mental-health issues, making it difficult to deliver effective and personalised services.[44] In addition, when attempting to gain housing support, offenders are often asked to repeat the same information to different people because of "unconnected case management systems."[45] One interviewee for this paper argued that the repetition of information can cause significant stress for an individual, particularly if it is about the repetition of a traumatic experience.

Creating a coherent data infrastructure, which allows public-sector organisations to easily and securely access relevant data is difficult. This is in part due to the inherent differences between data and information.[46] In healthcare, for example, information is passed on from patients to healthcare practitioners – and from one healthcare practitioner to another – who can use it to diagnose and treat. This information then gets codified and standardised and becomes data (see Figure 5).

Data can be more easily analysed as it is formatted in a specific way. It can, for example, allow comparisons to be drawn between the performance of one acute trust and another. Data can be found in the form of text, numbers, pictures, sound or video and, if taken out of context, might mean very little to public-service practitioners.[47] There is therefore an inherent tension between information which is context-specific and the desire to be able extrapolate and use that information outside of its context by converting it into data.

40 Ibid.
41 Connecting Care, *Bristol's Homeless Health Service | Case Study*, 2017.
42 Care Quality Commission, *Homeless Health Service Quality Report*, 2017
43 HM Inspectorate of Probation, *Transforming Rehabilitation: An Independent Inspection of the Arrangements for Offender Supervision*; National Audit Office, *Transforming Rehabilitation*, 2016; Public Accounts Committee, *Transforming Rehabilitation Inquiry*, 2016.
44 National Audit Office, *Mental Health in Prisons*, 2017, 45.
45 National Audit Office, Transforming Rehabilitation, 2016, 39.
46 Rob Wilson et al., 'New Development: Information for Localism? Policy Sense-Making for Local Governance', 296.
47 Ibid., 296–97.

Figure 5: The missing layer of data infrastructure
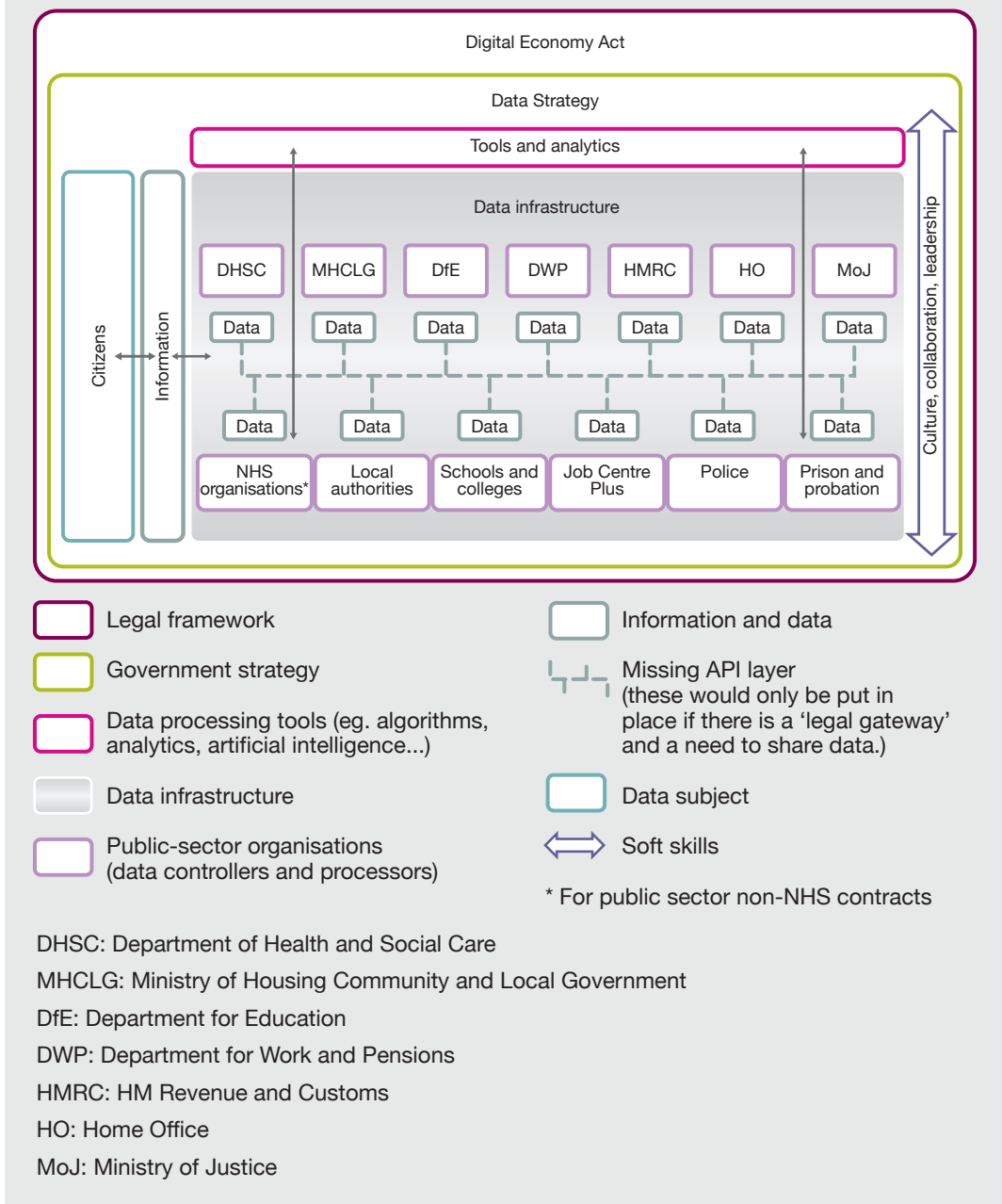
Source: *Reform* interviews.

As highlighted by the Open Data Institute, the creation of a clear data infrastructure would be one way to alleviate that tension.[48] Several interviews carried out for this paper argued that it is the missing layer from the Government's strategies. Government has focused on providing the legal framework and the tools and analytics but has missed the harder question of how to create an effective and secure data infrastructure to support its plans. Chapters 2-4 of this paper will focus on some of the constitutive elements of an effective data infrastructure.

---

48   Open Data Institute, *Using Open Data to Deliver Public Services*, 2018, 43; Open Data Institute, 'Principles for Strengthening Our Data Infrastructure', Webpage, 12 August 2016.

2
The data: sticking points

An effective and secure data infrastructure demands getting several key technical elements right. The inability to link or exchange information due to issues with the quality or type of data being shared prohibits effective data sharing. Technical barriers are closely related to other issues.[49] Inadequate data formats and standards, for example, may reflect a culture that places little emphasis on the importance of data sharing.[50] However, getting data collection, security and access right is critical to enable data to be shared within and across public services. This means collecting the right type of data in a consistent format, increasing its quality and creating a secure system to link data between organisations.

2.1 Data quality

Individual pieces of data must be presented in standard formats to enable sharing within and across services. Standards around the format of personal data can help create a common language, allowing information to be shared and understood within and across different systems.[51] Research and interviews for this paper have highlighted three main ways in which data quality can be increased: at the point of data collection, through better monitoring of data quality and standards within public-sector organisations and through data-curation-processes.

Minimising error at the point of data collection first requires rethinking the design of data systems and automating data-collection processes, to reduce human errors. The design of electronic health records system, for example, can have a strong impact on the quality of data collected.[52] Nevertheless, collection for purposes other than direct patient care – also known as secondary uses – can create a burden on frontline staff, especially where data quality can be unrelated to the needs of direct care. It is important to be aware of this tension when designing data-collection systems.

As highlighted by several interviews carried out for this paper, an awareness of the limitations datasets might have and a clear understanding of what the data is measuring, what it is not, and what it could be helpful for, is key. For example, the Department for Education's (DfE) pupil database collects data on exclusions but, prior to 2006, this did not include any reasons for exclusion, limiting what the data can tell us in that period.[53] *Reform* interviews also stressed that it is often the case that public servants will collect data and fail to consider that this data may be relevant or useful to another service. As a result, data that might seem less relevant to the running of that particular service is inputted with less care or sometimes ignored altogether. Several interviewees stated that this is, in part, a cultural issue as public bodies have not had to consider how this data may be used by other bodies and therefore solely focus on their own need.

Creating common standards, therefore, is problematic because different organisations are interested in different pieces of information. However, there are methods of bridging the gap between how different organisations hold data.[54] Departments can create synthetic datasets, or 'dummy data', which is structurally similar to the data they hold but obscures personal information to protect privacy.[55] This means when, for example, the DfE request data on child healthcare, the Department of Health and Social Care (DHSC) can send the DfE the dummy dataset. The DfE can then be more specific in their request, adhering to how the DHSC categorises its data. Implementing this system of 'dummy data' – also known

---

49   Deloitte, *New Technologies Case Study: Data Sharing in Infrastructure*, 2017.
50   Ibid.
51   James Cornford, Susan Baines, and Rob Wilson, 'Representing the Family: How Does the State "Think Family"?', *European Journal of Policitcs and Gender* 41, no. 1 (January 2013): 8–11.
52   W Rollason, K Khunti, and S de Lusignan, 'Variation in the Recording of Diabetes Diagnostic Data in Primary Care Computer Systems: Implications for the Quality of Care', *US National Library of Medicine National Institutes of Health* 17, no. 2 (2009); Simon de Lusignan et al., 'Call for Consistent Coding in Diabetes Mellitus Using the Royal College of General Practitioners and NHS Pragmatic Classification of Diabetes', *Informatics in Primary Care* 20, no. 2 (2012): 103–13.
53   Department for Education, *The National Pupil Database. User Guide*, 2015.
54   Ted Girard, 'Why Big Data Needs "Dummy Data"', *Nextgov*, 11 November 2014.
55   Ibid.

as synthetic data – would enable organisations to ask for the right data, helping organisations share data with different standards and encouraging data minimisation.[56]

Once data is collected, it is crucial to monitor its quality. There have been attempts to improve data monitoring within the public sector. NHS Digital produces a Data Quality Maturity Index, which aims to monitor data quality across the system.[57] However, it depends on voluntary submissions, meaning there is no consistent oversight of the quality of data collected within the NHS.[58] The ONS uses the UK Statistics Authority's Administrative Data Quality Assurance Toolkit for public-sector finances, which sets out the required quality assurance level of each administrative data source in government.[59] However, this level of robustness does not extend to other areas of public-sector data. The Government's 'Framework for Data Processing', included in the Data Protection Bill, could provide the right context to push for quality assurance across the public sector.

Once errors are embedded, any process of data curation is loaded with its own subjectivity.[60] Computational techniques are emerging to help address this subjectivity through communities, such as the discrimination-aware data mining. Algorithms also pose similar issues with bias. Some have argued that companies should opt into audits which test the biases of algorithms, and receive a seal of approval, or an O'Neil Risk Consulting & Algorithmic Auditing (ORCAA), if it passes.[61] The same stamp could be applied to test the quality of the initial data input, creating a more transparent system which recognises that, while data cannot be stripped of all biases, it can work to identify and manage them.[62] These organisations point to the importance of developing solutions to data quality issues through accounting for the biases and recognising real-world fairness challenges.[63]

Recommendation 1

Public-sector organisations should offer synthetic datasets, which they can share with others so that requests for data adhere to the right data standards in each organisation.

Recommendation 2

Within the Government's Framework for Data Processing, the Department for Digital, Culture, Media and Sport should create a Data Quality Assurance Toolkit and ensure that public-sector bodies submit data to be tested.

Recommendation 3

The Department for Digital, Culture Media and Sport should create a seal of approval, similar to the O'Neil Risk Consulting & Algorithmic Auditing (ORCAA), which indicates that data quality is satisfactory and that biases within datasets have been accounted for.

---

56   Ibid.
57   NHS Digital, 'Improving Data Quality Assurance', Webpage, 9 May 2017.
58   Ibid.
59   Office for National Statistics, 'Quality Assurance of Administrative Data Used in the UK Public Sector Finances: Feb 2017', Webpage, 21 February 2017.
60   Osonde Osoba and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence* (RAND Corporation, 2017), 19; Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data', *Big Data & Society* 4, no. 2 (December 2017).
61   ORCAA, 'O'Neil Risk Consulting & Algorithmic Auditing', Webpage, 2018.
62   Jessi Hempel, 'Want to Prove Your Business Is Fair? Audit Your Algorithm', *WIRED*, 9 May 2018.
63   Veale and Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data'.

2.2   Data linking

Within the public sector, various pieces of data are collected on citizens, which together form an individual's 'identity'.[64] Connecting this information effectively, so that someone's name matches their address, National Insurance number and medical history, for example, can be critical for providing the right services to the right people. One study, focusing on electronic healthcare data, argued that as the volume of data expands, linking data effectively is crucial to allow professionals to obtain trusted information about their patients.[65]

Currently, the lack of unified identity management can act as a barrier to the effective sharing of personal data. A number of interviewees said that there is no certainty that the right data is linked to the right people, with one predicting that at least 10 per cent of records in the public sector are linked to the wrong person. Errors in linking data correctly led to 505 inmates being released by mistake over the last decade to 2014-15.[66] Algorithms have been used to determine whether two sets of information belong to separate people or the same individual.[67] However, this is often not completely precise, and accuracy can depend on the context.[68] Interoperability issues and legacy systems act as significant barriers to data linking.

2.2.1   Interoperability

Data linking is infeasible if the systems used are not compatible. Issues of interoperability occur when multiple IT systems are unable to communicate with one another.[69] There are many examples of this across the public sector. The police continue to use two different national IT systems, which are incompatible: the police national computer and the police national database.[70] Within local forces, hundreds of incompatible systems are used. In 2014, for example, Britain's largest force, the Metropolitan Police Service, had 750 different systems in place.[71] Local bodies are often particularly hampered by ageing IT systems which, for the police, mean digital documents often need to be transformed back into hard copies, limiting the efficiency of services.[72] Twenty-three forces now use NicheRMS, a software system that unifies data-entry applications, but there are many forces which are yet to implement such technology to aid interoperability.[73] The Home Office National Automatic Number Plate Recognition Service offers another model, which includes scrutiny and oversight.[74]

These interoperability issues prevent information sharing. The National Audit Office's (NAO) report on Transforming Rehabilitation found a lack of information sharing between prisons and probation due to incompatible IT systems.[75] An Inspectorate report highlighted that "in only one-fifth of the cases was there evidence of information sharing between the responsible officer".[76] This lack of information sharing prevents the provision of real through-the-gate services in the justice system.

64   Maisie Borrows, Eleonora Harwich, and Luke Heselwood, *The Future of Public Service Identity: Blockchain* (Reform, 2017).
65   Richard E Gliklich, Nancy A Dreyer, and Michelle B Leavy, *Registries for Evaluating Patient Outcomes, 3rd Edition. A User's Guide* (Rockville: Agency for Healthcare Research and Quality, 2014).
66   BBC News, '"Hundreds of Inmates" Released in Error', 28 December 2015.
67   Gliklich, Dreyer, and Leavy, *Registries for Evaluating Patient Outcomes, 3rd Edition. A User's Guide*.
68   Ibid.
69   Department of Health, *Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England*, 2016, 49.
70   Alexander Babuta, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities* (RUSI, 2017).
71   Elizabeth Crowhurst, *Reforming Justice for the Digital Age* (The Police Foundation, 2017).
72   Ibid.
73   Babuta, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*.
74   Tony Porter, 'The ANPR Independent Advisory Group Is Now in Being!!', *GOV.UK*, 15 February 2018.
75   National Audit Office, *Transforming Rehabilitation*, 2016.
76   HM Inspectorate of Probation, *Transforming Rehabilitation: An Independent Inspection of the Arrangements for Offender Supervision*.

2.2.2 Dealing with the past

Legacy databases can further complicate information sharing. A legacy system, in the context of computing, refers to old computer systems, programming languages or application software that are still being used even though more up-to-date ways of operating are available.[77] When describing databases, legacy refers to a previous way in which information and data was collected and stored within an organisation. The discontinuation of a service or a change in a way a service is provided can create issues of legacy. Legacy databases are often inflexible and unable to adapt to changing needs. A NAO report on managing the risk of legacy ICT found that the Office of Fair Trading was unable to implement several recommendations from an efficiency and effectiveness review in April 2010, because the changes were not supported by the legacy databases.[78]

Attempts to deal with legacy systems have been haphazard. In the Home Office, the flagship Immigration Case Work programme was supposed to replace the legacy Casework Information Database and 20 other systems, but the programme was closed in 2013, having achieved little and costing £347 million.[79] In 2015, Whitehall announced the Crown Hosting programme, intended to map departments' legacy systems into an updated data centre, but take-up to the scheme was low.[80] The Department for Work and Pensions (DWP) intended to shift 250 of its systems to the data centre but ended up migrating just five.[81]

This is unsurprising considering the challenge of migrating databases away from legacy systems, which central government and departments seem to be underestimating. The structure of data in legacy systems, for example, is often different. As one paper identified, this difference is not just limited to table names, field names or attributes and sizes, but the types of databases are also often incompatible.[82] The technical skills required to map data may not be available and the risk of losing, or mis-translating sensitive data when mapping it across to new systems may not be worth taking for some organisations.[83] A survey by Experian found that 79 per cent of public-sector organisations in the US had an interest in abandoning legacy databases and updating their systems.[84] However, given the statutory obligation for public-sector organisations to continue to hold the data trail within legacy systems, abandoning them entirely is not possible.

2.2.3 Improving data linking

Improving data linking is partly about getting other elements 'right', such as the data standards and quality, which in turn can enable interoperability. It also begs a wider question around information flows within the public sector. Interviewees explained that public services collect data in a siloed fashion as they are only concerned with the specific data required for a specific service they wish to perform. This fosters issues of interoperability as the data does not follow the citizen journey through services. For example, when a crime is committed, the offender is separately evaluated by the police, then Crown Prosecution Service, courts and prisons, without looking at the offender journey by following the individual.[85] Changing the information flow can bring control back to the individual, by creating a more decentralised and user-centric approach to data sharing.[86] Innovative technologies can begin to create these opportunities. The shift from a siloed approach to focus on a trail that connects one person would radically improve data linking.

77 Sushma Velimeneti, *Data Migration from Legacy Systems to Modern Database* (St Cloud State University, 2016).
78 National Audit Office, *Managing the Risks of Legacy ICT to Public Service Delivery*, 2013.
79 National Audit Office, *Reforming the UK Border and Immigration System*, 2014.
80 Kat Hall, 'UK.Gov Still Drowning in Legacy Tech Because No One's Boarding Blighty's £700m Data Centre Ark', *The Register*, 23 January 2017.
81 Ibid.
82 Sushma Velimeneti, *Data Migration from Legacy Systems to Modern Database*.
83 Ibid.
84 Matthew Chase, 'The State of Data Management in the Public Sector in 2018', *Experian*, 8 February 2018.
85 Alexander Hitchcock and Sarah Timmis, *Crime and Information: Using Data and Technology to Transform Criminal-Justice Services* (Reform, 2018).
86 Thomas Hardjono, *Trust :: Data, A New Framework for Identity and Data Sharing*.

However, there are also technical solutions to be embraced within the current infrastructure to encourage interoperability and improve data linking. If the issue of standards is addressed, Application Programming Interfaces (APIs) can be overlaid on top of legacy systems to improve interoperability and enable data sharing (see Figure 6). In healthcare, Fast Healthcare Interoperability Resources (FHIR) creates a common standard, or language, that all health IT systems could use to interpret and process data.[87] FHIR demonstrates that, with a standardised system, APIs can be used in healthcare to increase interoperability.[88] Well-designed APIs, strategically deployed, have helped unlock digital transformation for private-sector organisations.[89] Amazon famously required all data and functionality to be available only through APIs.[90] It is thought that the public sector can follow suit. In the Government's *Transformation Strategy*, it listed opening up government services internally and externally through the use of APIs as a key priority by 2020.[91] Research suggests APIs could overcome data-sharing barriers because they can make data freely available to use within and between organisations, supporting interoperability, reducing costs and improving security.[92] However, the power of APIs can only be unleashed if there are proper standards and a clear data model in place.

Figure 6: What are Application Programming Interfaces (APIs)?

An Application Programming Interface (API) is a set of standard commands which allows applications to share data without developers having to share software code or write this code from scratch.[93] For example, the Twitter API is a web-based API that allows developers to interact and use Twitter data to create new applications.[94] For Government, an API can help to extend the reach of information held by public bodies and provide automated real-time updates to assist the building of new services.[95] For APIs to work effectively, however, it requires public organisations to use Open Standards to support software interoperability.[96]

In the longer term, public services must begin to recognise the importance of building interoperable systems from the start. Interviewees explained that current IT procurement rules allow companies to sell products to the public sector which are incompatible. This creates a "vendor lock-in" situation, where customers have little flexibility in choice of vendors as they have to choose products that are compatible with their original purchase.[97] To encourage competition and improve interoperability, procurement rules should make interoperability a prerequisite for competing companies, allowing customers to integrate their choices of the most appropriate products from different vendors.[98]

Recommendation 4

Technology vendors selling to public-sector bodies should ensure that their products are compatible with relevant Application Programming Interfaces (APIs), allowing this technology to overcome interoperability issues and government to change providers with ease.

87   Margaret Rouse, 'What Is FHIR (Fast Healthcare Interoperability Resources)?', SearchHealthIT, 30 October 2017.
88   Ibid.
89   Keerthi Iyengar et al., 'What It Really Takes to Capture the Value of APIs', Webpage, McKinsey & Company, (2018).
90   Kin Lane, 'The Secret to Amazons Success Internal APIs', *API Evangelist*, 12 January 2012.
91   Cabinet Office, *Government Transformation Strategy*.
92   Developer Program, "Introduction to APIs in Government", Webpage, (2018).
93   GOV.UK, 'Application programming interfaces (APIs)', Webpage, 16 December 2016.
94   Jonathan Freeman, 'What Is an API? Application Programming Interfaces Explained', Webpage, 9 May 2018
95   Gray Brooks, 'APIs in Government', Blog, DigitalGov, 30 April 2013.
96   Daniel Appelquist, 'Our Approach to APIs: The Basics - Technology at GDS', Blog, GOV.UK, 20 June 2016.
97   Stacy A Baird, 'Government Role and the Interoperability Ecosystem', *Journal of Law and Policy for the Information Society* 5, no. 2 (2012).
98   Ibid.

Recommendation 5

Moving forward, it should be mandatory for any system procured within the public sector to adopt open standards, encouraging competition and improving interoperability by avoiding vendor lock-in situations.

2.3 Actionability: it's not just about the data

Overcoming these technical issues will help in building the systems and tools to make data more actionable – meaning that insights derived from data can be converted into action.[99] The sharing of personal data is only one step in the design of more effective services tailored to the needs of the population.

Without well-designed systems and tools to read and analyse data, public servants are unable to reap the benefits of data.[100] In its examination of the Transforming Rehabilitation reforms, the NAO has argued that the various ICT systems used to assess and allocate offenders "are cumbersome and require repeated data re-entry."[101] In addition, one interviewee for this paper stated that even though data-sharing agreements meant that they were able to access different datasets, there was no single simple interface to compare this information. Instead, they were forced to open several datasets simultaneously – meaning that it is difficult to link the information effectively.

To become valuable, the analysis of data must be able to inform a decision.[102] One way of achieving this is by improving the infrastructure that enables integration of the data.[103] In addition to data access, it is essential to improve the way software used by public servants is designed.[104]

99   Nevena Dragicevic, 'Three Lessons for Innovating with Data in the Public Sector', Blog, 24 October 2017.
100 Sue Bowman, 'Impact of Electronic Health Record Systems on Information Integrity: Quality and Safert Implications', *Perspectives in Health Information Management* 10 (October 2013).
101 National Audit Office, *Transforming Rehabilitation*, 2016, 8.
102 Tom Symons, *Datavores of Local Government: Using Data to Make Services More Personalised, Effective and Efficient* (Nesta, 2016) 23.
103 Ibid., 6.
104 Rachel Becker, 'How Badly Designed Electronic Health Records Can Put Patients in Danger', *The Verge*, 28 March 2018; Sue Bowman, 'Impact of Electronic Health Record Systems on Information Integrity: Quality and Safert Implications'; Ben Shneiderman, Catherine Plaisant, and Bradford W Hesse, 'Improving Healthcare with Interactive Visualization', *Computer* 46, no. 5 (May 2013).

3
Building
trustworthiness

Creating a trusted and secure system where public servants are confident to share personal data and the public is confident their data will be shared securely should be at the heart of any data-sharing agreement and system.[105] Trust is important both between citizens and government and between organisations within and across government domains. This trust can at times be damaged by the lack of clarity over what constitutes public benefit for sharing data. Being able to share data at scale using the internet has brought about new threats to the security and privacy of personal information, as data can be hacked. Cybersecurity is crucial to the construction of a trustworthy data infrastructure as no public-sector organisation should share data unless it is confident of its provisions to keep it secure.

3.1   Grey areas

In specific contexts, the need to share data between public-sector organisations is irrefutable. For example, "where there is a clear and determinate risk of major harm, such as an imminent terrorist attack or serious abuse of a child"[106]. Nonetheless, there are many grey areas where the initial public benefit for sharing personal data is ambiguous or the benefit only appears to be clear for one of the parties involved.[107]

Data-sharing agreements can occur between public services that have different aims, meaning that data could be used for a purpose that is in contradiction with duties of one of the services involved.[108] For example, sharing data between services whose primary purpose is to benefit specific citizens (such as health and social services) and uphold a duty of confidence[109]; and services whose aim is to protect the public from harm and sanction in cases where there is a breach to the law (such as police and criminal justice services) can create professional, moral and ethical problems. In April 2018, the Health and Social Care Committee raised "serious concerns" about the Memorandum of Understanding (MOU), which allowed patient data held by NHS Digital to be shared with the Home Office, arguing that it breached confidentiality rules and patient trust.[110] Between January and November 2016, the Home Office made 8,127 requests for patient details to trace people breaking immigration rules, resulting in 5,854 people being tracked by immigration enforcement.[111] Here, the Home Office's use of patient data was at odds with its initial purpose, raising concerns that it would undermine doctor-patient trust and create tension with the duty of confidentiality that doctors are required to uphold.[112]

There can at times be disagreements about the type of data (i.e. personal identifiable, de-identified or pseudonymised – see glossary for definitions) some public services should have access to and what they would like to have access to. The type of data shared between public bodies can create an ethical dilemma, with certain services or organisations wanting access to different gradients of personal information. For example, medConfidential have reported that NHS England have granted a legal exemption to pass personal identifiable data to various commissioning bodies, which can be used for administrative purposes, auditing, service planning and targeting and providing evidence to assess the effectiveness of services.[113] Arguably, there is no need for that data to be personal identifiable and it would benefit from a certain degree of anonymisation.

105 Pentland et al., 'Towards the Internet of Trusted Data'.
106 Perri 6, Bellamy, and Raab, 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management', 470.
107 Kaela Scott, *Data for Public Benefit: Balancing the Risks and Benefits of Data Sharing* (Involve, Carnegie UK Trust, Understanding Patient Data, 2018).
108 Denis Campbell, 'NHS Will No Longer Have to Share Immigrants' Data with Home Office', *The Guardian*, 9 May 2018; May Bulman, 'Public Health England Warns of "Serious Risk" over Home Office Data Sharing', *The Independent*, 29 April 2017.
109 Sebastian Porsdam Mann, Julian Savulescu, and Barbara J. Sahakian, 'Facilitating the Ethical Use of Health Data for the Benefit of Society: Electronic Health Records, Consent and the Duty of Easy Rescue', *Phil. Trans. R. Soc.* A.374, no. 2083 (28 December 2016).
110 Health and Social Care Committee, *Oral Evidence - Memorandum of Understanding on Data-Sharing between NHS Digital and the Home Office*, 2018.
111 May Bulman, 'Public Health England Warns of "Serious Risk" over Home Office Data Sharing'.
112 Denis Campbell, 'NHS Will No Longer Have to Share Immigrants' Data with Home Office'.
113 MedConfidential, 'More Information | MedConfidential', Webpage, 2018.

3.2 Trust and public opinion

According to the National Data Guardian's 2017 report, "no project, however worthy of its aims, will succeed unless those holding, sharing and using data act in a way that inspires and retains public trust."[114] Although this reference applies specifically to the healthcare context, the trustworthiness of government's mechanisms for holding, sharing and using data are important across public services. However, public trust in how the Government handles data remains low. The Royal Statistical Society has highlighted the existence of a 'data trust deficit' in society, meaning trust in institutions to use data appropriately is lower than trust in them in general.[115] Advances have been made in certain policy areas such as health and social care.[116] However, Government has not yet managed to establish a framework across public-sector organisations to safeguard public's trust. Ensuring the provenance and governance of data and giving individuals recourse can help to build public trust.

3.2.1 The weight of past mistakes

The recent history of large-scale attempts at data sharing has not helped to secure confidence in how personal data is used by government. In 2014, the care.data programme, designed to allow anonymised primary care health records to be shared outside the NHS, had to be paused after loss of public trust.[117] Personal data was used without clearly explaining to the public its intent, leading to concerns about informed consent, security and the default "opt-in" system.[118] The programme officially ended after the second Caldicott report was published calling for greater safeguards around the sharing of patient data and for "clarity" on the future of care.data.[119] Interviewees agreed that, while care.data could have improved medical research, the covert approach to using personal data meant, in the words of one, "the harm was greater than good".

Data breaches are relatively common across government and can further reduce confidence. The NAO recorded 8,995 data breaches across the 17 largest government departments in 2014-2015.[120] Another report found that Britain's local governments were hit by almost 100 million cyber-attacks in the last five years, while one in four councils' systems were successfully breached.[121] According to the National Cyber Security Centre chief, part of the issue is that many organisations are "simply bad at doing the basics right"[122], something exacerbated by low budgets and underinvestment.[123] A recent Accenture survey found that 58 per cent of respondents across six countries, including the UK, said that high-profile cyber-attacks in 2017, including WannaCry and Petya, had a direct impact on their confidence in government's ability to protect their data.[124] Another survey found that many are still wary of recent public-security attacks, with 61 per cent expressing concern about how secure their data is held, and 37 per cent worried over the lack of control they have.[125] The ICO supported this, recording that only 36 per cent of citizens feel that their data is properly secured.[126] This suggests data breaches impact public confidence.

---

114 National Data Guardian, *Impact and Influence for Patients and Service Users* (Department of Health, 2017).
115 Royal Statistical Society, Royal Statistical Society Research on Trust in Data and Attitudes toward Data Use/Data Sharing, 2014.
116 National Data Guardian, *Information: To Share or Not to Share? Information Governance Review* (Department of Health, 2013); National Data Guardian for Health and Care, *Review of Data Security, Consent and Opt-Outs*, 2016; National Data Guardian, *Impact and Influence for Patients and Service Users*.
117 The Royal Society, *Data Governance : Landscape Review*, 2017.
118 Tjeerd-Pieter van Staa et al., 'Big Health Data: The Need to Earn Public Trust', BMJ : British Medical Journal, 14 July 2016.
119 National Data Guardian for Health and Care, *Review of Data Security, Consent and Opt-Outs.*
120 National Audit Office, *Protecting Information across Government*, 2016.
121 Big Brother Watch, *Cyber Attacks in Local Authorities*, 2018.
122 Nick Ismail, '"When Not If" the UK Suffers a Very Serious Cyber Attack – NCSC Chief Ciaran Martin', *Information Age*, 23 January 2018.
123 it governance, 'Public Sector', Webpage, 2018.
124 Ger Daly, 'Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security', *Nextgov*, 6 April 2018.
125 Chris Doutney, 'Do Citizens Trust the Government to Handle Their Personal Data?', Webpage, 2018.
126 Information Commissioner's Office, *Information Commissioner's Office- Trust and Confidence in Data* (ComRes, 2017).

3.2.2 Opaque data trails

The way in which data is used and by whom affects levels of trust and confidence. Figures published recently by *Reform* showed that, while trust in government is higher than private companies, just 9 per cent of people feel that the Government has their best interests at heart when data sharing, and only 15 per cent are confident that government organisations would deal well with a cyber-attack.[127] Research by the Royal Statistical Society suggest that support for data sharing varies in different contexts.[128] For example, over seven in ten think that all hospitals and GPs should be able to access health records for patients' care. However, 84 per cent say that health records should not be sold to private-healthcare companies to make money for government.[129] As new technologies introduce innovative ways of storing and sharing information, public anxiety over what is happening with citizens' personal data can increase.[130] Questions are raised, not just over who is holding information and whether it is secure, but also over precisely what is being done with personal data.[131]

These questions do not always receive adequate answers from Government.[132] Research suggests that the more information people have, the more comfortable they are with wider uses of data.[133] However, interviewees agreed that Government has tended to discuss data sharing behind closed doors without engaging the public in how they wanted their data to be used. Research by the Wellcome Trust found that people were largely unaware of how data is already being used within the NHS and confused about whether data is identifiable and what anonymisation means in practice.[134] An ICO survey found that just 8 per cent of UK adults feel they have good understanding of how their personal data is made available to third parties and 6 per cent had heard of the EU's General Data Protection Regulation.[135] Without improving this dialogue, it will remain a challenge to increase public trust in data sharing.

3.3 Trust and organisational culture

Building trust between organisations to share information is just as important as building trust with the public. Creating organisations in which the culture is geared towards sharing data - through trusted relationships and the right skills - is needed to ensure data is shared securely, transparently and efficiently.

3.3.1 Scepticism in the public sector

While there are examples of trusted relationships across the public sector, there are mixed attitudes toward data sharing and multi-agency work in many organisations.[136] Often organisations develop different working cultures and practices which creates apprehension towards sharing within and across policy domains. The NAO found that one of the issues with the Transforming Rehabilitation programme was the creation of "new organisations with different incentives".[137] For example, many junior staff managing high-risk offenders in the National Probation Service, felt their contracts with Community Rehabilitation Companies, designed to handle low-risk offenders, were not providing them with necessary information and had become too focused on their commercial interests as opposed to the best interests of offenders.[138] A recent Nesta paper on

---

127 Reform and Deloitte, *Citizens, Government and Business. The State of the State 2017-18*, 2017.
128 Royal Statistical Society, *Royal Statistical Society Research on Trust in Data and Attitudes toward Data Use/Data Sharing.*
129 Ibid.
130 British Academy and Royal Society, *Data Management and Use: Governance in the 21st Century*, 2017.
131 Mustafa Suleyman and Ben Laurie, 'Trust, Confidence and Verifiable Data Audit', DeepMind, 9 March 2017.
132 British Academy and Royal Society, *Data Management and Use.*
133 Ibid.
134 Wellcome Trust, *The One-Way Mirror: Public Attitudes to Commercial Access to Health Data* (Ipsos MORI, 2016).
135 Information Commissioner's Office, *Information Commissioner's Office- Trust and Confidence in Data.*
136 Centre of Excellence for Information Sharing, *Overcoming Cultural Barriers to Information Sharing within Regulatory Services*, 2016.
137 National Audit Office, *Transforming Rehabilitation*, 2016.
138 Ibid.

'data-driven local government' showed that in six of eight local councils studied, a lack of appetite for data-informed decisions and working was a barrier.[139]

Challenging the status quo within any working culture can provoke resistance, particularly when there is anxiety about getting data sharing wrong. The Centre of Excellence for Information Sharing found in their research that a fear of getting information sharing wrong meant a reluctance to share at all.[140] One report on the role of information sharing in helping tackle gang and youth violence identified a fear of being exposed for holding poor quality data as a powerful barrier to sharing.[141] This can be exacerbated by the weight of legal liability on some public servants. The British Medical Association's General Practitioners Committee has warned GPs in the past not to sign up to data-sharing schemes where they leave GPs open to legal challenges.[142] Without the right working culture to encourage best practice towards data sharing in the public sector, increasing trust between organisations and the decisions made about data will remain challenging.

3.3.2 Skills gap: tech and policy

The Government's *Transformation Strategy* highlighted "embedding digital skills throughout government"[143] as key to better data sharing. Frontline staff do not all need to be experts in data handling, however they do need to understand systems around them to let them do their job and meet user needs. Where skills gaps exist, trust between organisations can decrease.

Skills vary greatly at different levels of public services, limiting data sharing in some key sectors. Several interviewees highlighted a particularly worrying skills gap within areas of local government, where tight budgets can impede best practice. One council said it was only because they "happened to have the skills in house" that any system to share data securely could be initiated. These concerns are supported by research. A recent Nesta paper on 'data-driven local government' showed that the concept of data-led innovation is unfamiliar to many employees.[144] Lack of skills and capacity were flagged as an issue in six of the eight councils studied and half the case studies reported that there had been a gap between the aspirations of the project and the technical expertise and skills of their staff.[145] The Royal Statistical Society have highlighted that access to good-quality local data would increase trustworthiness in data sharing, but this can only be facilitated through a mixture of skills, expertise and basic understanding.[146]

The General Data Protection Regulation (GDPR) has introduced Data Protection Officers (DPOs) within government departments and public-sector organisations.[147] The role of the DPO is to help public organisations monitor internal compliance with the GDPR, advise on data-protection obligations and act as a contact point for data subjects.[148] The introduction of this role is a good start in creating awareness of the problems with data handling in government, and could help with the skills gap in government.

3.4   Establishing a new relationship

According to Dame Fiona Caldicott, the National Data Guardian, there should be 'no surprises' to citizens in how their data is used and citizens should have a choice about how their data is used.[149] Considering public trust is currently being undermined by opacity and error, it would help to create a clearer system for sharing data in which the

139 Tom Symons, *Wise Council: Insights from the Cutting Edge of Data-Driven Local Government* (Nesta, 2016).
140 Centre of Excellence for Information Sharing, *Overcoming Cultural Barriers to Information Sharing within Regulatory Services.*
141 Centre of Excellence for Information Sharing, *Benefits and Challenges in Tackling Gang and Youth Violence*, 2015.
142 Alex Matthews-King, 'Local GP Data Sharing Schemes "Open Practices up" to Legal Challenges', Pulse, 6 May 2015.
143 Cabinet Office, *Government Transformation Strategy.*
144 Tom Symons, *Wise Council: Insights from the Cutting Edge of Data-Driven Local Government.*
145 Ibid.
146 Royal Statistical Society, *Data Manifesto*, 2016.
147 Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, 193.
148 Ibid.
149 National Data Guardian, *Impact and Influence for Patients and Service Users*, 9.

public is involved in decisions and can monitor how their personal data is used. Improving the transparency and auditability of how data is used within government, therefore, is a necessary first step to increasing public trust in data sharing.

3.4.1 Continuous public engagement

Issues of trustworthiness can partly be overcome by creating a system for data sharing that delivers transparency. Considering attitudes towards data sharing are time and context dependent,[150] engaging citizens and clearly explaining when and why data is used can help build confidence.

There are already projects aiming to bridge the gap between data use and public knowledge. The Wellcome Trust's 'Understanding Patient Data' has been set up to explain how health and care data is used.[151] In their assessment of public attitudes to data sharing, the Wellcome Trust reported that if the public knew more about the processes and safeguarding of data sharing, they would be more open and trusting to these arrangements – a conclusion that was reached in several interviews for this paper.[152] By explaining the importance of data sharing to citizens, and by including the public in the process of inputting data to support the delivery of services, one interviewee argued that it would give citizens a greater stake in creating successful public services, motivating them to input the right information and correct anomalies. In addition, interviewees for this paper highlighted the importance of better communicating the outcomes of data-sharing agreements between public-sector bodies.

Recommendation 6

Government departments should identify and support initiatives like Understanding Patient Data in all policy areas, supporting organisations if they need to properly engage citizens and understand how they want their data to be used across public services.

3.4.2 Verifiable data audit

In the context of increasing trust and confidence in using data, auditability of how data is used and by whom is increasingly important. This data about data, such as the context, meaning, format and collection date, is referred to as 'metadata'.[153] Metadata provides an audit trail, which can be used to verify what is happening with each individual piece of personal data.[154]

Auditability can only increase confidence if transparency is accompanied with evidence of proper security. Interviewees noted that low funding makes it difficult for organisations to get a good level of security, especially in local government and smaller institutions. While issues of cybersecurity are out of the scope of this research, encrypting data (see glossary for definition) properly and ensuring it is secure is fundamental.

New technology has transformed the potential of data audits. DeepMind have used this concept to develop an accurate and secure system of tracing data. Its 'Verifiable Data Audit' is working to give theoretical mathematical assurance about what is happening with data in real-time, to ensure it is only used as it should be.[155] Every time an entry is added, a "cryptographic hash" is generated, which ensures that every time data is changed, it is traced.[156] Medicalchain is another platform, which uses blockchain

150 Royal Statistical Society, *Royal Statistical Society Research on Trust in Data and Attitudes toward Data Use/Data Sharing*.
151 Understanding Patient Data, 'Understanding Patient Data', Web Page, 2018.
152 Wellcome Trust, *The One-Way Mirror: Public Attitudes to Commercial Access to Health Data*, 13.
153 British Academy and Royal Society, *Data Management and Use*.
154 Ibid.
155 Suleyman and Laurie, 'Trust, Confidence and Verifiable Data Audit'.
156 Ibid.

technology to give users conditional access to different parts of the healthcare system, such as hospitals and doctors, and ensures every interaction with personal data is auditable, transparent and secure.[157] Whether these technocratic approaches are sufficient to reassure individuals remains to be seen.

Digital data audits can also provide a more flexible framework around citizen consent, which is critical to ensuring a transparent data-sharing model. Dynamic consent connects services and individuals through personalised, digital platforms, putting people at the heart of decision making.[158] This is enabled through technology that can securely encrypt sensitive data and inform individuals when data is shared with third-parties, improving transparency and public trust.[159]

The difficulty is knowing the optimum form of engagement. Limited time and resources mean lengthy juries or focus groups to engage the public are not practical.[160] Similarly, few interviewees advocated constantly notifying individuals every time their data was used. According to one, it is "neither feasibly nor sensible" because bombarding vulnerable individuals with notifications, when often they may find engagement with services difficult in the first place, is counterproductive. Instead, there needs to be spaces where people can find out how data has been used, why and by whom, in language they can understand.[161]

Making this a reality in the public sector requires a level of knowledge and understanding among public servants. The Government's *Transformation Strategy* is right to highlight the need to support non-digital specialists in understanding the potential of new or different ways of working.[162] However, its method for doing this is unclear. The Centre of Excellence for Information Sharing recommended training in a number of case studies as key to enabling data sharing in local government.[163] For example, when launching Dorset's Information Sharing Charter, healthcare practitioners said training would help them understand the legalities of sharing data, and the Centre recommended mandatory training and cross-agency joint-training after speaking to people on the ground.[164] Ensuring that public servants have a base level of understanding to navigate the use of data is key to enabling these new ways of working with data.

Recommendation 7

All government departments should prepare to develop audit trails which track how data is used to ensure every interaction with personal data is auditable, transparent and secure.

Recommendation 8

Government should, in partnership with the Information Commissioner's Office, investigate and publicise the optimum training needed to familiarise public servants with the handling of personal data, to reduce the fear of using and sharing personal data.

---

157 Medicalchain, *Medicalchain Whitepaper 2.1*, 2018, 1.
158 Jane Kaye et al., 'Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks', *European Journal of Human Genetics* 23, no. 2 (2015).
159 Ibid.
160 British Academy and Royal Society, *Data Management and Use*.
161 Ibid.
162 Cabinet Office, *Government Transformation Strategy*.
163 See Centre of Excellence for Information Sharing, *How to Build a MASH Using Information Sharing as Your Building Block*, 2016; Centre of Excellence for Information Sharing, *Information Sharing in Greater Manchester: Wigan's SharetoCare Programme*, 2016; Centre of Excellence for Information Sharing, *Better Together: Implementing a New Information Sharing Charter for Dorset In-Depth Report*, 2016.
164 Centre of Excellence for Information Sharing, *Better Together: Implementing a New Information Sharing Charter for Dorset In-Depth Report*.

Legal complexities

The current legal framework surrounding data sharing and data governance is often described as being highly complex and evolving.[165] Some major developments have occurred in the last year: the EU's General Data Protection Regulation (GDPR) as implemented by the 2018 Data Protection Act, plus the Digital Economy Act (DEA). These legislations sit on top of pre-existing legal frameworks, which can create a nebulous system for public-sector organisations to navigate.[166] This complexity creates uncertainty within public bodies as to who is accountable when data is shared. The Law Commission argues that this "uncertainty is often identified as one of the main obstacles preventing public bodies from sharing data."[167]

It is unclear what drives this complexity and whether it is a necessary part of the data-sharing process. According to one interviewee there is "no appetite for changing the law" because legal barriers are critical to avoid "fishing expeditions" with citizens' personal data. As the Law Commission identifies, it is ambiguous whether this complexity is a result of inadequacies in the legal system or a reflection of the various policy concerns and cultural uncertainty underlying data sharing, which may create unnecessary legal obstacles.[168] Furthermore, it could be that setting up gateways for specific data-sharing instances is not scalable or sustainable, demonstrating the importance of a data infrastructure approach.

4.1 Legal gateways

Every time information is shared, public-sector organisations must go through the process of creating, or finding the right legal 'gateway' to enable sharing in a secure way.[169] Prior to the DEA, sharing information required finding an explicit gateway through which information can be disclosed or received, usually for a specific purpose.[170] For example, social security data obtained for an authorities Housing Benefit scheme could not be re-used for another function unless the law provides a gateway for this.[171] One interviewee explained that creating new gateways to allow for the sharing of information can take any time from three months to three years, with an average time of about 18 months. This puts a significant break on allowing personal data to be accessed when it is needed.

The DEA has worked to change this, by establishing "clear and robust" legal gateways, which enable public authorities to share relevant information more easily.[172] However, some interviewees still voiced concerns around legal gateways and its impact remains to be seen. The legal complexity also requires a desire within organisations to understand legal frameworks, which is not always present. Government has issued guidance on the laws around data sharing,[173] but there also needs to be a change in mindset. Nesta's recent case studies on data sharing within local councils showed that, for each council examined, it was possible to legally share data in accordance with current legislation, and that it was a case of encouraging this practice within the organisation.[174] However, with continuing question marks over accountability when data-sharing agreements are made, this remains difficult.

4.2 Keeping with the times

Legislation has at times struggled to keep pace with the rapidly evolving way in which data is being used. According to Baroness O'Neill in the House of Lord's second reading of the Data Protection Bill, concepts change meaning over time and in different contexts.[175]

165 Law Commission, *Data Sharing between Public Bodies*, 2014; Eleonora Harwich and Kate Laycock, *Thinking on Its Own: AI in the NHS* (Reform, 2018).
166 The Royal Society, *Data Governance : Landscape Review*.
167 Law Commission, *Data Sharing between Public Bodies*.
168 Ibid.
169 Ibid.
170 Ministry of Justice, *Public Sector Data Sharing: Guidance on the Law*, 2010.
171 Department for Work and Pensions, *Guidance for Local Authorites on the Use of Social Security Data*, 2014.
172 HM Government, *Digital Economy Act 2017*.
173 Ministry of Justice, *Public Sector Data Sharing: Guidance on the Law*.
174 Tom Symons, *Wise Council: Insights from the Cutting Edge of Data-Driven Local Government*.
175 House of Lords, 'Data Protection Bill, Second Reading' (2017).

Notions of accountability, agency, consent, privacy and ownership are becoming more difficult to maintain, due to new approaches to data collection and use in the digital age.[176] The GDPR is aiming to find a solution to this, strengthening data-protection laws to try and safeguard people's data against the rapidly changing technological landscape.[177]

However, there are already concerns in the ability of new legislation to keep with the times.[178] For example, it is vital legislation is well-connected to underlying technologies for collecting, processing and using data, but keeping pace with huge leaps forward in machine learning and artificial intelligence (AI) in recent years is no easy task.[179] Research by the British Academy and Royal Society highlighted that, in this fast-moving landscape, governance challenges need to be addressed "in a timely manner" if the overall system of governance for data management and data use is to maintain both public trust and efficacy.[180]

As public bodies are governed by public law, they have a fundamental advantage as AI and whatever comes after AI is considered. The high standards for data processing by public bodies are clear, and widely understood, which makes it easier for suppliers to meet them than might be the case for other sectors of the economy which are not used to requiring clarity on their actions.

4.3   Demystifying legislation

The constantly evolving ways in which data is used suggests that the legal landscape will continue to adapt. This is certainly what has been seen with new legislation in the past year. Therefore, it is important to provide mediums which demystify legislation for those trying to understand how to use data within the legal landscape.

There are already websites which aim to demystify legislation around data. Information Commissioner's Office (ICO) has online guidance for companies and individuals trying to navigate legislation and understand their rights when it comes to handling personal data.[181] The website breaks the guidance down by sector, with guidance for local government differing from the education sector, for example.[182] It has recorded some podcasts with the Centre of Excellence for Information Sharing discussing the cultural challenges facing specific areas of the public sector in light of the GDPR.[183] However, the Centre of Excellence has ceased to exist as its funding has not been renewed.[184]

This idea could go further to ensure there is a clear body of information which public-sector leaders can go to understand the legal basis for their data-sharing agreements and instill confidence in leaders to share data. This could resemble the NHS's data security and protection toolkit.[185] The resource could sit between the work of the two organisations, by producing clear documents on the technicalities of legislation, but also providing clear case studies with examples of best practice catered to the public-sector bodies.

Recommendation 9

The Information Commissioner's Office should continue to partner with specialist organisations, like the former Centre of Excellence for Information Sharing, who help demystify legislation, with resources and case studies specifically catered to public-sector bodies.

176 British Academy and Royal Society, *Data Management and Use*.
177 GOV.UK, 'Government to Strengthen UK Data Protection Law', Press Release, 7 August 2017.
178 The Royal Society, *Data Governance : Landscape Review*.
179 Ibid.
180 British Academy and Royal Society, *Data Management and Use*.
181 Information Commissioner's Office, 'Home', Webpage, 2018.
182 Information Commissioner's Office, 'For Organisations', Webpage, 2018.
183 Information Commissioner's Office, 'Local Government', Webpage, 23 April 2018.
184 Stephen Curtis, 'Changes to the Centre', Webpage, Centre of Excellence for Information Sharing, June 2018.
185 NHS Digital, 'Data Security and Protection Toolkit', Webpage, 2018.

5
The enablers

Harnessing the power of data in the public sector requires a new approach to how data is understood and used. Creating a new model, which will allow organisations to overcome barriers to data sharing and build on government promises outlined in its *Transformation Strategy*, requires clear leadership and a collaborative approach. Overcoming these issues will take a concerted effort that looks to the long term and extends beyond the political cycle. For real 'transformation', there needs to be a clear leadership structure, and a proper clarification of the roles of local authorities, regions and government departments in getting the data infrastructure right.

5.1   Leadership and accountability

Creating the right leadership structure is not easy.[186] Despite the existence of legal gateways to share data between public-sector bodies there are still areas which remain unclear such as who is accountable for data pooled between different organisations. A new accountability and leadership model is needed to set out clearly these roles and responsibilities. Opportunities are arising to redirect leadership through new structures, such as the Data Advisory Board, and new positions, such as the Chief Data Officer. These opportunities could be used to help foster collaboration through strong leadership that extends across departments and beyond the political cycle.

To promote data sharing and data standards, Government should build on its commitment to establish a Data Advisory Board that will "align efforts to make best use of data across government" by 2020.[187] The Advisory Board's broad objectives are to look at cross-departmental data strategies and to accelerate current data programmes across government.[188] While this development should be lauded, accelerating current initiatives is not enough. For the Board to be effective, its objective should be to tackle the various challenges facing data sharing in the public sector, and to offer recommendations for cross-departmental strategies. To do this, the Advisory Board should ensure that it includes a representative from each department to share responsibility and promote data standards across government. This would help to improve engagement and would ensure collective responsibility.

In addition to the Data Advisory Board, the *Transformation Strategy* pledged to appoint a new Chief Data Officer, which would work alongside the DPOs within government departments.[189] This role, which has been vacant since September 2015[190], aims to establish cross-government data standards and oversee the Government's data strategy. The sharing of individual's personal data should be added to the role's remit, to ensure there is a role for specifically helping with data sharing across siloed departments.

Recommendation 10

The new Data Advisory Board should focus its attention on tackling the difficult challenges stopping effective multi-agency data sharing. The Advisory Board should include a representative from each department to ensure collective responsibility.

---

186 medConfidential, *Digital and Data in Government*, 2017.; Tom Symons and Emma Prest, 'The Data Evolution: New Tools to Help Organisations Get More from Their Data', Nesta, 26 January 2017.
187 Cabinet Office, *Government Transformation Strategy*, 10.
188 Bouchard, 'Manzoni Leads UK Chief Data Officer Hunt in Wider Reform Drive', News Release, Government Computing Network, 27 March 2017.
189 Cabinet Office, *Government Transformation Strategy*.
190 Bouchard, 'Manzoni Leads UK Chief Data Officer Hunt in Wider Reform Drive'.

Recommendation 11

Data-sharing policy should be included in the remit of the Chief Data Officer, so there is a specific individual championing best practice towards data sharing across siloed departments.

To support the Data Advisory Board and the Chief Data Officer, clear leadership from the top of the Civil Service is needed to drive through change. Since April 2018, the responsibility for data sharing, data ethics, open data and data governance was transferred to the Department for Digital, Culture, Media and Sport (DCMS) from the Cabinet Office's Government Digital Service.[191] Although the scope and powers of the new Centre for Data Ethics and Innovation remains unclear, demonstrated by its launch of an Open Consultation in June 2018[192], its influence risks being confined to DCMS. Instead, clear leadership from the Cabinet Office through the Data Advisory Board and Chief Data Officer to ensure that data-sharing principles reach across departments.

Recommendation 12

Leadership on the sharing of individuals' personal data should come from the Cabinet Office rather than the Department for Digital, Culture, Media and Sport to help to ensure that the Government's data-sharing strategy has influence that reaches across departments.

5.2   The regional/national balance

In addition to national leadership and accountability, local government can play an important role in promoting data sharing across the public sector. Developing data-sharing agreements and standards at a local level can provide space to test projects and for these to be scaled if successful.

Local data-sharing agreements should be created to meet a local need. They can, however, provide an infrastructural and standards template for larger-scale data-sharing agreements. The *Wachter Review* argues that promising local and regional efforts to promote interoperability and data sharing should be built upon.[193] It recommends that national funding could be linked to local projects that demonstrate they are "adequately prepared to succeed."[194] Building on successful local projects can help avoid over-investing in projects with little chance of success and focus on mapping best practice on a wider scale. For example, setting regional standards for how data is collected and recorded regarding homeless people would help the 13 regions to create larger policy strategies that are informed by local contexts. In addition, this would mean that there was less variation in data standards across the country, which would make it easier for this data to be shared from region-to-region. Here, the principle of subsidiarity is key. Data should be collected and used at the level nearest the issue at hand.

There are promising examples where local projects could be scaled-up across the country. Calderdale Metropolitan Borough Council, for example, received £10,000 from the Local Government Association (LGA) for its data-sharing agreement focused on children's services. This agreement gives local authorities an opportunity to self-assess children's services, in line with Ofsted's framework. The LGA argues, however, that this is

191 Theresa May MP, 'Machinery of Government Changes: Written Statement' (HCWS609, 29 March 2018).
192 Department for Digital, Culture, Media & Sport, 'Centre for Data Ethics and Innovation Consultation', Open Consultation, GOV.UK, 13 June 2018.
193 Department of Health, *Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England*, 4.
194 Ibid., 5–6.

"not just a Calderdale nor Yorkshire & Humber issue but a national one."[195] Therefore, Calderdale is providing a "template model" that will be tested in this area and could be scaled nationally.[196] According to the LGA, by taking this approach, the Calderdale Metropolitan Borough Council will be able to share examples of best practice.

There are, of course, times where top-down initiatives are needed to ensure that data can be shared across the country. The National Pupil Database, for example, collects information for all state schools across the country such as pupils' test and exam results, in addition to their progression across each key stage. By ensuring that there are standards for how this information is recorded, it makes it possible – albeit a "significant undertaking" – to match data on a national scale. By creating national standards for how information is collected and recorded, it enables the Department for Education and third parties to conduct research, produce statistics and inform national education policy.

However, for many cases, successful examples of data sharing within local areas should have the potential to be scaled-up. One interviewee argued that the aim of data sharing across public services is not to see "a thousand flowers that bloom badly." In other words, rather than having several data-sharing projects with limited potential, the objective is to enable successful projects that could be expanded across the country.

Recommendation 13

Local government should play an important role in the establishment of data standards and infrastructure. By giving local areas space to try and test data-sharing arrangements, it will help to demonstrate which projects are successful and could be scaled up regionally and nationally.

---

195 Local Government Association, 'LGA Data Experts Grants Support Better Use of Local Data Mini Projects', News Release, Local Government Association, 11 January 2017.
196 Ibid.

Conclusion

The internet and new technologies have opened up many opportunities to share data digitally. As more data is collected and generated, there is huge potential to analyse and share data to improve effectiveness and citizen interaction with public services.[197] The current cost of not sharing data is high.[198] It can lead to gaps in service provision, repetition of information – which can sometimes be traumatic for service users, and poor outcomes. Data sharing is crucial to improve service delivery and outcomes, and its benefits can be espoused by all.

However, the public sector has not yet managed to maximise these benefits. Currently, there are uncoordinated attempts to share data that do not have the appropriate data infrastructure to allow public-sector organisations to access the data that they need to deliver the best outcomes. For the Government to live up to its ambition of creating joined-up public services centred around people's needs, it will need to provide standards and protocols and focus on the construction of a stronger infrastructure around data.

This is increasingly important as the public sector faces new and emerging issues of ethics, privacy and consent.[199] Scandals, such as the use of data by Cambridge Analytica, have highlighted how data can be exploited and used for purposes that it was not meant for, meaning users can lose control and systems can be hacked.[200] In this context, every attempt at sharing data must be clear about how that data will be kept secure.

Security is critical to building trust in data sharing, both between public-sector organisations and with the public. In the past, trust has been damaged by the lack of clarity over why personal data is shared and with whom. Creating new relationships, through stronger dialogue with the public and greater transparency across organisations about how data is used, will help increase confidence and help organisations reap the benefits of data sharing.

Driving this type of change within government will need strong leadership as creating an effective data infrastructure is not a quick and easy feat. It will take time to tackle the various technical barriers, provide guidance to practitioners and create the right culture within public-sector organisations to foster the appropriate sharing of data. This will require collaboration between the centre and local areas, across different sectors, and between the state and citizens to create the ecology for the co-production of the data infrastructure.

It is, however, a challenge worth facing. Overcoming these issues will help government 'get data right' and design programmes to better join-up public services and put citizens at their centre. With the right infrastructure, and leadership driving change, the result could be truly transformative.

---

197 British Academy and Royal Society, *Data Management and Use*.
198 Kerina H. Jones et al., 'The Other Side of the Coin: Harm Due to the Non-Use of Health-Related Data', *International Journal of Medical Informatics* 97, no. Supplement C (January 2017): 43–51; Eleonora Harwich, Alexander Hitchcock, and Elaine Fischer, *Faulty by Design: The State of Public-Service Commissioning* (*Reform*, 2017).
199 British Academy and Royal Society, *Data Management and Use*.
200 Zoe Kleinman, 'Cambridge Analytica: The Story so Far', *BBC News*, 21 March 2018.

Appendix

In February, *Reform* held a research roundtable on 'The sharing of personal data between public services'. The roundtable served as a discussion to present and challenge some of the thinking behind *Reform*'s research project on the sharing of personal data between public-sector bodies. The team was at an early stage of research and wanted to benefit from the insights and advice of attendees as to how the project could evolve moving forward.

The event

The event was attended by ten experts in the field. The *Reform* team gave a 20-minute presentation on the initial findings of the research. The team then chaired an hour-long discussion on the themes of the paper. The discussion was semi-structured and covered the general structure and scope of the project; the benefits of sharing data; technical, cultural and legal barriers; and potential solutions.

Attendees

George Batchelor	Director, Edge Health
Dr Louise Bennett	Co-chair, The Privacy and Consumer Advisory Group
Vasja Bocko	Chief Executive Officer, Iryo
Ben Evans	Data Hub Programme Manager, Newham Council
Yvonne Gallagher	Director of Digital Value for Money, National Audit Office
Eleonora Harwich	Head of Digital and Technological Innovation, *Reform*
Dr Luke Heselwood	Researcher, *Reform*
Imogen Heywood	Engagement Manager, Centre of Excellence for Information Sharing (has since changed position)
Kaj Siebert	Chief Technology Officer, Social Finance UK
Jovian Smalley	Group Manager – Engagement (Public Services), Information Commissioner's Office
Sarah Timmis	Researcher, *Reform*
Prof Rob Wilson	Chair of Information Systems Management and Director, Centre for Knowledge Innovation Technology and Enterprise, Newcastle University Business School, Newcastle University
Amy Woolfson	Research Assistant, Law Commission

Glossary

Anonymised data: data "about individuals but with identifying details removed".[201]

Audit trail: A record of everyone who has looked at or changed a record, why and when they did so and what changes they made.[202]

Consent (and its different forms): "approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily."[203]
Explicit Consent: "It can be given in writing or verbally, or conveyed through another form of communication such as signing." [204] **Implied consent:** "applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed." [205]

Database: a database is a collection of information that is organised so that it can be easily accessed, managed and updated.

> Should it be centralised or decentralised? Where should data be stored?

Data architecture: this is the overall environment of data and includes frameworks, models, standards, policies, data management, data quality, unstructured data etc.

Data controller: "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."[206]

Data linkage: "joining of two or more administrative or survey datasets using individual reference numbers/identifiers or statistical methods such as probabilistic matching."[207]

Data model: this is the equivalent of a blueprint of an actual data structure. It shows the business concepts and how they relate to each other. It is the abstract model that both organises data and standardises how they relate to one another.

> How should new models be created from various databases? When the information is already gathered, how can new data models ensure they are robust, safe and accurate?

Data processor: "any person (other than an employee of the data controller) who processes the data on behalf of the data controller."[208]

Data standards: these are the rules by which data are described and recorded. In order to share data properly, the format and the meaning of the data must be standardised.

> How should we be collecting and categorising data? Why is the quality of data so important? What standards should we be imposing on data and how rigid need these be?

Data subject: "means an individual who is the subject of personal data".[209]

Data warehouse: a central repository of integrated data from one or more disparate sources.[210]

---

201 NHS Digital, 'How We Look after Information', Webpage, 2017.
202 National Data Guardian, *Information: To Share or Not to Share? Information Governance Review*.
203 Health & Social Care Information Centre, *A Guide to Confidentiality in Health and Social Care*, 2013, 7.
204 Ibid.
205 Ibid.
206 Information Commissioner's Office, *Guide to Data Protection*.
207 Dean Machin, *Data and Public Policy – Trying to Make Social Progress Blindfolded*, Social Mobility and Child Poverty Commission, 2015, 20.
208 Information Commissioner's Office, *Guide to Data Protection*.
209 Ibid.
210 Spotless data, 'Exploring Data Warehouses and Data Quality', Webpage, 2018.

De-identified data: data for which personal identifying information (i.e. name, date of birth, NHS number…) has been removed.

Encrypted data: the translation of data into another form, or code, so that only people with access to a secret key or password can read it.[211]

Information governance: the way in which organisations management the way information and data are handled to ensure it is legal, secure, efficient and effective.[212]

Legal gateways: "by which information can be disclosed or received for particular purposes. Such gateways may be permissive (creating a discretionary power to disclose or receive data) or mandatory (requiring data to be transferred in certain circumstances)."[213]

Personal data: Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.[214]

Personal identifiable data: "containing details that identify individuals". [215]

Pseudonymised data: "data about individuals but with identifying details (such as name or NHS number) replaced with a unique code."[216] This can allow reidentification by using a separate database which contains the unique code and identifiable data.

Population/aggregate data: "anonymised information grouped together so that it doesn't identify" individuals. [217]

211 Nate Lord, 'What Is Data Encryption?', *Digital Guardian*, 15 January 2018.
212 National Data Guardian, *Information: To Share or Not to Share? Information Governance Review*.
213 Ministry of Justice, *Public Sector Data Sharing: Guidance on the Law*, 5.
214 Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*.
215 NHS Digital, 'How We Look after Information'.
216 NHS Digital, 'How We Look after Information'.
217 Ibid.

Bibliography

Appelquist, Daniel. 'Our Approach to APIs: The Basics – Technology at GDS'. Blog. GOV. UK, 20 June 2016.

Babuta, Alexander. *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*. RUSI, 2017.

Baird, Stacy A. 'Government Role and the Interoperability Ecosystem'. *Journal of Law and Policy for the Information Society* 5, no. 2 (2012).

Bate, Alex. *The Troubled Families Programme (England)*. CBP 07585. House of Commons Library, 2016.

BBC News. '"Hundreds of Inmates" Released in Error', 28 December 2015, sec. UK.

Becker, Rachel. 'How Badly Designed Electronic Health Records Can Put Patients in Danger'. *The Verge*, 28 March 2018.

Bell, Professor Sir John. *Life Sciences Industrial Strategy – A Report to the Government from the Life Sciences Sector*. HM Government, 2017.

Big Brother Watch. *Cyber Attacks in Local Authorities*, 2018.

Borrows, Maisie, Eleonora Harwich, and Luke Heselwood. *The Future of Public Service Identity: Blockchain*. *Reform*, 2017.

Bouchard, Luc. 'Manzoni Leads UK Chief Data Officer Hunt in Wider Reform Drive'. News Release. Government Computing Network, 27 March 2017.

Bowman, Sue. 'Impact of Electronic Health Record Systems on Information Integrity: Quality and Safert Implications'. *Perspectives in Health Information Management* 10 (October 2013).

Bracken, Mike. 'Government as a Platform: The next Phase of Digital Transformation'. *Government Digital Service*, 29 March 2015.

Brooks, Gray. 'APIs in Government'. Blog. DigitalGov, 30 April 2013.

Bulman, May. 'Public Health England Warns of "Serious Risk" over Home Office Data Sharing'. *The Independent*, 29 April 2017.

Cabinet Office. *Government Transformation Strategy*, 2017.

———. *Modernising Government*. London: Stationary Office, 1999.

———. *Transformational Government: Enabled by Technology*, 2005.

Cabinet Office, and Government Digital Service. *Better Use of Data in Government*, 2016.

Campbell, Denis. 'NHS Will No Longer Have to Share Immigrants' Data with Home Care Quality Commission. *Homeless Health Service Quality Report*, 2017.

———. 'NHS Will No Longer Have to Share Immigrants' Data with Home Office'. *The Guardian*, 9 May 2018.

Centre of Excellence for Information Sharing. *Sharing Health Data to Improve Outcomes for Families and Children: Staffordshire Case Study*, 2016.

———. *Benefits and Challenges in Tackling Gang and Youth Violence*, 2015.

———. *Better Together: Implementing a New Information Sharing Charter for Dorset In-Depth Report*, 2016.

———. *How to Build a MASH Using Information Sharing as Your Building Block*, 2016.

———. *Information Sharing in Greater Manchester: Wigan's SharetoCare Programme*, 2016.

———. *Overcoming Cultural Barriers to Information Sharing within Regulatory Services*, 2016.

———. 'How Information Sharing Is Improving Help for Troubled Families.' Webpage, 2018.

Chase, Matthew. 'The State of Data Management in the Public Sector in 2018'. *Experian*, 8 February 2018.

Combe, Colin. 'Observations on the UK Transformational Government Strategy Relative to Citizen Data Sharing and Privacy'. *Transforming Government: People, Process and Policy* 3, no. 4 (October 2009): 394–405.

Cornford, James, Susan Baines, and Rob Wilson. 'Representing the Family: How Does the State "Think Family"?' *European Journal of Policitcs and Gender* 41, no. 1 (January 2013): 8–11.

Connecting Care. *Bristol's Homeless Health Service | Case Study*, 2017.

Crowhurst, Elizabeth. *Reforming Justice for the Digital Age*. The Police Foundation, 2017.

Curtis, Stephen. 'Changes to the Centre'. The Centre of Excellence for Information Sharing, June 2018.

Daly, Ger. 'Citizens Support Increased Data-Sharing and Technology Innovation to Enhance Security'. Nextgov, 6 April 2018.

Davenport, Cheryl. *Integrating Care and Health Information across Leicester, Leicestershire and Rutland*, 2015.

Deloitte. *New Technologies Case Study: Data Sharing in Infrastructure*, 2017.

de Lusignan, Simon, Khaled Sadek, Helen McDonald, Pete Horsfield, Norah Hassan Sadek, Aumran Tahir, Terry Desombre, and Kamlesh Khunti. 'Call for Consistent Coding in Diabetes Mellitus Using the Royal College of General Practitioners and NHS Pragmatic Classification of Diabetes'. *Informatics in Primary Care* 20, no. 2 (2012): 103–13.

Department for Digital, Culture, Media and Sport. 'Centre for Data Ethics and Innovation Consultation'. Open Consultation. GOV.UK, 13 June 2018.

———. *UK Digital Strategy 2017*, 2017.

Department for Education. *The National Pupil Database. User Guide*, 2015.

Department for Work and Pensions. *Guidance for Local Authorites on the Use of Social Security Data*, 2014.

Department of Health. *Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England*, 2016.

Department of Health, Department for Communities and Local Government, Local Government Association, and NHS England. "Section 1: Population Segmentation, Risk Stratification and Information Governance." In *How to Guide: The BCF Technical Toolkit*, Ed. The Better Fund, 2014.

Developer Program, "Introduction to APIs in Government." Webpage, 2018.

Doutney, Chris. 'Do Citizens Trust the Government to Handle Their Personal Data?' Webpage, 2018.

Dragicevic, Nevena. 'Three Lessons for Innovating with Data in the Public Sector'. Blog. Nesta, 24 October 2017.

Dunleavy, Patrick. 'The Future of Joined-up Public Services 2020', 2010, 34.

Freeman, Jonathan. 'What Is an API? Application Programming Interfaces Explained'. Webpage, 9 May 2018.

Gilklich, Richard E, Nancy A Dreyer, and Michelle B Leavy. *Registries for Evaluating Patient Outcomes, 3rd Edition. A User's Guide*. Rockville: Agency for Healthcare Research and Quality, 2014.

Girard, Ted. 'Why Big Data Needs "Dummy Data"'. *Nextgov*, 11 November 2014.

GOV.UK, 'Application programming interfaces (APIs)'. Webpage, 16 December 2016.

———. 'Government to Strengthen UK Data Protection Law'. Press Release, 7 August 2017.

Green, Bob, Mary-Ann Bruce, Peter Finn, Alison Wright, David Daniel, Dr Jane Povey, and Dean Repper. *Independent Review of Deaths of People with a Learning Disability or Mental Health Problem in Contact with Southern Health NHS Foundation Trust April 2011 to March 2015*. Mazars, 2015.

Gold, Sarah. 'Data Sharing in the Government Transformation Strategy', IF, 15 February 2017.

Hall, Kat. 'UK.Gov Still Drowning in Legacy Tech Because No One's Boarding Blighty's £700m Data Centre Ark'. *The Register*, 23 January 2017.

Hardjone, Thomas. *Trust: Data, A New Framework for Identity and Data Sharing*. Visionnary Future, 2016.

Harwich, Eleonora, Alexander Hitchcock, and Elaine Fischer. *Faulty by Design: The State of Public-Service Commissioning*. *Reform*, 2017.

Harwich, Eleonora, and Kate Laycock. *Thinking on Its Own: AI in the NHS*. *Reform*, 2018.

Health and Social Care Information Centre. *A Guide to Confidentiality in Health and Social Care*, 2013.

Health and Social Care Committee. *Oral Evidence - Memorandum of Understanding on Data-Sharing between NHS Digital and the Home Office*, 2018.

Hempel, Jessi. 'Want to Prove Your Business Is Fair? Audit Your Algorithm'. *WIRED*, 9 May 2018.

Hitchcock, Alexander, and Sarah Timmis. *Crime and Information: Using Data and Technology to Transform Criminal-Justice Services*. *Reform*, 2018.

HM Government, *Digital Economy Act 2017*.

HM Inspectorate of Probation. *Transforming Rehabilitation: An Independent Inspection of the Arrangements for Offender Supervision*, 2016.

HM Revenue and Customs. *Sharing and Publishing Data for Public Benefit*, 2013.

House of Lords. Data Protection Bill, Second Reading (2017).

Information Commissioner's Office. *Data Sharing Code of Practice*, 2011.

———. 'For Organisations'. Webpage, 2018.

———. *Guide to Data Protection*, 2017.

———. *Guide to the General Data Protection Regulation (GDPR)*, 2018.

———. 'Home'. Webpage, 2018.

———. *Information Commissioner's Office- Trust and Confidence in Data*. ComRes, 2017.

———. 'Local Government'. Webpage, 23 April 2018.

Ismail, Nick. '"When Not If" the UK Suffers a Very Serious Cyber Attack – NCSC Chief Ciaran Martin'. *Information Age*, 23 January 2018.

it governance. 'Public Sector'. Webpage, 2018.

Iyengar, Keerthi, Somesh Khanna, Srinivas Ramadath, and Daniel Stephens. 'What It Really Takes to Capture the Value of APIs'. Webpage. McKinsey & Company, (2018).

Johnstone, Dr Androulla. *Independent Investigation into the Care and Treatment Provided to Mr X, Ms Y and Mr Z by the Dorset HealthCare University NHS Foundation Trust*. Health and Social Care Advisory Service, 2015.

Jones, Kerina H., Graeme Laurie, Leslie Stevens, Christine Dobbs, David V. Ford, and Nathan Lea. 'The Other Side of the Coin: Harm Due to the Non-Use of Health-Related Data'. *International Journal of Medical Informatics* 97, no. Supplement C (January 2017): 43–51.

Kaye, Jane, A Edgar, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. 'Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks'. *European Journal of Human Genetics* 23, no. 2 (2015).

Kleinman, Zoe. 'Cambridge Analytica: The Story so Far'. *BBC News*, 21 March 2018.

Lane, Kin. 'The Secret to Amazons Success Internal APIs'. *API Evangelist*, 12 January 2012.

Law Commission. *Data Sharing between Public Bodies*, 2014.

Local Government Association. 'LGA Data Experts Grants Support Better Use of Local Data Mini Projects'. News Release. Local Government Association, 11 January 2017.

Local Safeguarding Children Board. *Serious Review Case: Baby Peter*, 2009.

Lord, Nate. 'What Is Data Encryption?' *Digital Guardian*, 15 January 2018.

Machin, Dean. *Data and Public Policy – Trying to Make Social Progress Blindfolded*, Social Mobility and Child Poverty Commission, 2015, 5.

Manzoni, John. 'Big Data in Government: The Challenges and Opportunities'. Speech, 21 February 2017.

Matthews-King, Alex. 'Local GP Data Sharing Schemes "Open Practices up" to Legal Challenges'. *Pulse*, 6 May 2015.

medConfidential. *Digital and Data in Government*, 2017.

———. 'More Information | MedConfidential'. Webpage, 2018.

Medicalchain. *Medicalchain Whitepaper 2.1*, 2018.

Ministry of Justice. *Public Sector Data Sharing: Guidance on the Law*, 2010.

———. *Transforming Rehabilitation: A Strategy for Reform*, 2013.

National Audit Office. *Managing the Risks of Legacy ICT to Public Service Delivery*, 2013.

———. *Mental Health in Prisons*, 2017.

———. *Personalised Commissioning in Adult Social Care*, 2016.

———. *Protecting Information across Government*, 2016.

———. *Reforming the UK Border and Immigration System*, 2014.

———. *Transforming Rehabilitation*, 2016.

———. *Transforming Rehabilitation*, 2016.

National Data Guardian for Health and Care. *Impact and Influence for Patients and Service Users*. Department of Health, 2017.

———. *Information: To Share or Not to Share? Information Governance Review*. Department of Health, 2013.

National Data Guardian for Health and Care. *Review of Data Security, Consent and Opt-Outs*, 2016.

NHS Digital. 'Data Security and Protection Toolkit'. Webpage, 2018.

———. 'How We Look after Information'. Webpage, 2017.

———. 'Improving Data Quality Assurance'. Webpage, 9 May 2017.

NHS England. *Five Year Forward View*, 2014.

———. *Using Case Finding and Risk Stratification: A Key Service Component for Personalised Care and Support Planning*, 2015.

NHS South Central and West. 'Risk Stratification Tools in Somerset • South, Central and West CSU'. Webpage, 2018.

Office for National Statistics. 'Quality Assurance of Administrative Data Used in the UK Public Sector Finances: Feb 2017'. Webpage, 21 February 2017.

Open Data Institute. 'Principles for Strengthening Our Data Infrastructure'. Guidance. Open Data Institute, 12 August 2016.

———. *Using Open Data to Deliver Public Services*, 2018.

ORCAA. 'O'Neil Risk Consulting & Algorithmic Auditing'. Webpage, 2018.

Osonde, Osoba, and William Welser IV. *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*. RAND Corporation, 2017.

Pentland, Alex, David Shrier, Thomas Hardjono, and Irving Wladawsky-Berger. 'Towards the Internet of Trusted Data'. In *Trust :: Data, A New Framework for Identity and Data Sharing*, Ed. Thomas Hardjono, David Shrier, and Alex Pentland. Visionnary Future, 2016.

Perri 6, Christine Bellamy, and Charles Raab. 'Information-Sharing Dilemmas in Public Services: Using Frameworks from Risk Management'. *Policy & Politics* 38, no. 3 (July 2010): 465–81.

Porsdam Mann, Sebastian, Julian Savulescu, and Barbara J. Sahakian. 'Facilitating the Ethical Use of Health Data for the Benefit of Society: Electronic Health Records, Consent and the Duty of Easy Rescue'. *The Royal Society Publishing* 374, no. 2083 (November 2016).

Porter, Tony. 'The ANPR Independent Advisory Group Is Now in Being!!' *GOV.UK*, 15 February 2018.

Public Accounts Committee. *Transforming Rehabilitation Inquiry*, 2016.

Pugh, Rachel. 'The GP Practice Sharing Data to Transform Care for Homeless People'. *The Guardian*, 22 February 2017.

Reform, and Deloitte. *Citizens, Government and Business. The State of the State 2017-18*, 2017.

Roland, Martin, and Gary Abel. 'Reducing Emergency Admissions: Are We on the Right Track?' *BMJ* 345 (18 September 2012).

Rollason, W, K Khunti, and S de Lusignan. 'Variation in the Recording of Diabetes Diagnostic Data in Primary Care Computer Systems: Implications for the Quality of Care'. *US National Library of Medicine National Institutes of Health* 17, no. 2 (2009).

Rouse, Margaret. 'What Is FHIR (Fast Healthcare Interoperability Resources)?' SearchHealthIT, 30 October 2017.

Royal Statistical Society. *Data Manifesto*, 2016.

———. *Royal Statistical Society Research on Trust in Data and Attitudes toward Data Use/Data Sharing*, 2014.

Scott, Kaela. *Data for Public Benefit: Balancing the Risks and Benefits of Data Sharing*. Involve, Carnegie UK Trust, Understanding Patient Data, 2018.

Shneiderman, Ben, Catherine Plaisant, and Bradford W Hesse. 'Improving Healthcare with Interactive Visualization'. *Computer* 46, no. 5 (May 2013).

Sidebotham, Peter, Marian Brandon, Sue Bailey, Pippa Belderson, Jane Dodsworth, Jo Garstang, Elizabeth Harrison, Ameeta Retzer, and Penny Sorensen. *Pathways to Harm, Pathways to Protection: A Triennial Analysis of Serious Case Reviews 2011 to 2014*. Department for Education, 2016.

Social Finance. *Commissioning for Outcomes across Children's Services and Health and Social Care*, 2015.

———. *New Insights into Improving Outcomes for At-Risk Youth*, 2016.

Spotless data. 'Exploring Data Warehouses and Data Quality'. Webpage, 2018.

Suleyman, Mustafa, and Ben Laurie. 'Trust, Confidence and Verifiable Data Audit'. DeepMind, 9 March 2017.

Symons, Tom. Datavores of Local Government: Using Data to Make Services More Personalised, Effective and Efficient. Nesta, 2016.

———. *Wise Council: Insights from the Cutting Edge of Data-Driven Local Government*, (Nesta, 2016).

Symons, Tom, and Emma Prest. 'The Data Evolution: New Tools to Help Organisations Get More from Their Data'. Nesta, 26 January 2017.

The Royal Society and British Academy. *Data Management and Use: Governance in the 21st Century*, 2017.

The Royal Society. *Data Governance : Landscape Review*, 2017.

Theresa May MP. 'Machinery of Government Changes: Written Statement'. HCWS609, 29 March 2018.

Tjeerd-Pieter van Staa, Ben Goldacre, Iain Buchan, and Liam Smeeth. 'Big Health Data: The Need to Earn Public Trust'. *BMJ : British Medical Journal*, 14 July 2016.

Understanding Patient Data. 'Understanding Patient Data'. Web Page, 2018.

Veale, Michael, and Reuben Binns. 'Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data'. *Big Data & Society* 4, no. 2 (December 2017).

Velimeneti, Sushma. *Data Migration from Legacy Systems to Modern Database*. St Cloud State University, 2016.

Wellcome Trust. *The One-Way Mirror: Public Attitudes to Commercial Access to Health Data*. Ipsos MORI, 2016.

Wilson, Rob, James Conford, Sue Baines, and John Mawson. 'New Development: Information for Localism? Policy Sense-Making for Local Governance'. *Public Money & Management* 31, no. 4 (May 2011).