| | |
|---|---|
| **Title:**<br>Introduction of new powers for bodies to disclose identified data for the purpose of combating fraud against the public sector<br>**IA No:**<br>**Lead department or agency:**<br>Cabinet Office<br>**Other departments or agencies:**<br>HMRC, DWP, HO, DfT, CLG, DH and MoJ | **Impact Assessment (IA)**<br>**Date:** 09/02/2016<br>**Stage:** Development/Options<br>**Source of intervention:** Domestic<br>**Type of measure:** Primary legislation<br>**Contact for enquiries:**<br>Firoze Salim<br>(firoze.salim@cabinetoffice.gov.uk) |

## Summary: Intervention and Options

**RPC Opinion:** Not Applicable

| Cost of Preferred (or more likely) Option | | | | |
|---|---|---|---|---|
| **Total Net Present Value** | **Business Net Present Value** | **Net cost to business per year** (EANCB on 2009 prices) | **In scope of One-In, Two-Out?** | **Measure qualifies as** |
| £m | £m | £m | Yes/No | In/Out/zero net cost |

**What is the problem under consideration? Why is government intervention necessary?**

Public sector estimates of losses due to fraud is estimated to be at least £20.3bn. Wider use of data sharing would improve the prevention, detection and investigation of fraud by aiding better targeting and risk-profiling of potentially fraudulent individuals. However, there are currently legal barriers which place significant burdens on organisations which wish to share data. This limits the ease in establishing data sharing agreements between public bodies.

**What are the policy objectives and the intended effects?**

The policy objective is to reduce the cost of fraud to the public sector (and by extension to the taxpayer) by increasing flexibility and the reducing the time and complexity involved in establishing the sharing of data. We intend to confer a permissive power on public bodies listed in a schedule in the legislation to authorise data sharing between them for the prevention, detection, investigation or prosecution of fraud against the public sector. Creating a clear purposive gateway will provide public bodies with assurance as to what is legally permissable and in turn allow greater flexibility for Government to act more quickly to combat fraud.

**What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)**

1) Option 1 – Do nothing: The status quo would be maintained, whereby specific statutory gateways are created when there is a need for them.
2) Option 2 - Introduce new legisation that enables Public Authorities to share any data for any purpose, if there is a public benefit and is within the bounds of the Data Protection Act and Human Rights Act.
3) Option 3 - Non-legislative work to change cultural boundaries: simpler guidance, brokerage of data-sharing agreements or other such provision.
4) Option 4 (preferred option) - Introduce new legislation which enables the sharing of data between public authorities within clearly set constraints (who can share, what they can share and for what purpose). This option reduces data sharing complexity and cost as Public Authorities use the purposive gateway rather than individual gateways. It also balances this benefit with the protection afforded to the individual.

**Will the policy be reviewed?** It will be reviewed. **If applicable, set review date:** Month/Year

| | | | | | |
|---|---|---|---|---|---|
| Does implementation go beyond minimum EU requirements? | | | Yes / No / N/A | | |
| Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base. | **Micro** No | **< 20** No | **Small** No | **Medium** No | **Large** No |
| What is the $CO_2$ equivalent change in greenhouse gas emissions? (Million tonnes $CO_2$ equivalent) | | | **Traded:** N/A | **Non-traded:** N/A | |

***I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.***

Signed by the responsible SELECT SIGNATORY: ..... Date: .....

# Summary: Analysis & Evidence

Policy Option 1

**Description:** Do nothing

**FULL ECONOMIC ASSESSMENT**

| Price Base Year | PV Base Year | Time Period Years | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low:** Optional | **High:** Optional | **Best Estimate:** |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | Optional | | Optional | **Optional** |
| **High** | Optional | | Optional | **Optional** |
| **Best Estimate** | | | | |

**Description and scale of key monetised costs by 'main affected groups'**

In line with impact assessment guidance the do nothing option has zero costs or benefits as impacts are assessed as marginal changes against the do nothing baseline.

**Other key non-monetised costs by 'main affected groups'**

In line with impact assessment guidance the do nothing option has zero costs or benefits as impacts are assessed as marginal changes against the do nothing baseline.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | Optional | | Optional | **Optional** |
| **High** | Optional | | Optional | **Optional** |
| **Best Estimate** | | | | |

**Description and scale of key monetised benefits by 'main affected groups'**

In line with impact assessment guidance the do nothing option has zero costs or benefits as impacts are assessed as marginal changes against the do nothing baseline

**Other key non-monetised benefits by 'main affected groups'**

In line with impact assessment guidance the do nothing option has zero costs or benefits as impacts are assessed as marginal changes against the do nothing baseline.

| Key assumptions/sensitivities/risks | **Discount rate** | |
|---|---|---|

**BUSINESS ASSESSMENT (Option 1)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OITO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** | **Benefits:** | **Net:** | Yes/No | IN/OUT/Zero net cost |

# Summary: Analysis & Evidence

Policy Option 2

**Description:** Providing for a broad, Government-wide presumption to share data through legislating

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low:** Optional | **High:** Optional | **Best Estimate:** 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

N/A

**Other key non-monetised costs by 'main affected groups'**

It is expected that public sector bodies affected by the legislative change will face one-off familiarisation and training costs associated with the change in legislation. Public sector bodies will also incur administrative costs associated with an increased volume of data sharing requests – this is expected to be most significant under this option as it has the broadest scope for sharing data. However, it is expected that any data sharing burden would be at least partially offset by benefits associated with reduced likelihood and cost of fraud (see below).

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

N/A

**Other key non-monetised benefits by 'main affected groups'**

Public sector bodies will benefit from a decrease in the administrative costs of sharing data (i.e. staff time in researching or establishing legal data sharing gateways). The public sector will be better able to prevent, detect and investigate fraud leading to a reduced cost of fraud enabled through public sector bodies' ability to share data more quickly.

Key assumptions/sensitivities/risks **Discount rate**

The key risk of a legislative change lies in the possibility of future legal challenge with respect to the Data Protection Act or the Human Rights Act. This is most significant under this option as it enables a wide range of data sharing. Related to this, there is a risk in data loss and associated personal costs to citizens as well as reduced trust in government. A further risk is in incorrect use of data.

**BUSINESS ASSESSMENT (Option 2)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OITO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** | **Benefits:** | **Net:** | No | NA |

# Summary: Analysis & Evidence

Policy Option 3

**Description:** Non-legislative work to change the culture around data sharing in the public sector

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low:** Optional | **High:** Optional | **Best Estimate:** 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

N/A

**Other key non-monetised costs by 'main affected groups'**

Public sector bodies will face one-off costs related to the development and implementation of a culture change/training programme. This would involve training delivered to staff who are or could be involved in data sharing. Assuming a successful shift to increasing the level data sharing within the existing legal framework, public sector bodies will also face ongoing administrative costs associated with sharing data, but it is expected that these would be at least partially offset by benefits associated with reduced fraud.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

**Other key non-monetised benefits by 'main affected groups'**

Assuming a successful shift to increase data sharing within the existing legal framework, public sector bodies will benefit from a decrease in the administrative costs of sharing data (i.e. staff time in researching or establishing legal data sharing gateways where gateways already exist). The public sector will be better able to prevent, detect and investigate fraud leading to a reduced cost of fraud enabled through public sector bodies' ability to share data more quickly. The magnitude of these benefits is expected to be lower than under options 2 and 4.

Key assumptions/sensitivities/risks

**Discount rate**

**BUSINESS ASSESSMENT (Option 3)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OITO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** | **Benefits:** | **Net:** | No | NA |

# Summary: Analysis & Evidence

Policy Option 4

**Description:** Constrained powers to share data for specific purposes within specified but flexible groups

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2015 | PV Base Year 2015 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low:** Optional | **High:** Optional | **Best Estimate:** 0 |

| COSTS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised costs by 'main affected groups'**

**Other key non-monetised costs by 'main affected groups'**

It is expected that public sector bodies affected by the legislative change will face one-off familiarisation and training costs associated with the change in legislation. Public sector bodies will also incur administrative costs associated with an increased volume of data sharing requests – these are expected to be lower than under option 2 as data sharing is limited to instances where data is used to detect fraud. Again, it is expected that any data sharing burden would be at least partially offset by benefits associated with reduction in fraud.

| BENEFITS (£m) | Total Transition (Constant Price) | Years | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| **Low** | **Optional** | | **Optional** | Optional |
| **High** | **Optional** | | **Optional** | Optional |
| **Best Estimate** | **0** | | **0** | 0 |

**Description and scale of key monetised benefits by 'main affected groups'**

**Other key non-monetised benefits by 'main affected groups'**

Public sector bodies will benefit from a decrease in the administrative costs of sharing data (i.e. staff time in researching or establishing legal data sharing gateways). The public sector will be better able to prevent, detect and investigate fraud leading to a reduced cost of fraud enabled through public sector bodies' ability to share data more quickly.

Key assumptions/sensitivities/risks **Discount rate**

The key risk of a legislative change lies in the possibility of future legal challenge with respect to the Data Protection Act or the Human Rights Act. Related to this, there is a risk in data loss and associated personal costs to citizens as well as reduced trust in government. A further risk is in incorrect use of data in policy-making.

**BUSINESS ASSESSMENT (Option 4)**

| Direct impact on business (Equivalent Annual) £m: | | | In scope of OITO? | Measure qualifies as |
|---|---|---|---|---|
| **Costs:** | **Benefits:** | **Net:** | No | NA |

## Evidence Base (for summary sheets)

Problem under consideration

In 2012, the National Fraud Authority put the loss to the UK economy from fraud at £73 billion, with approximately £20.3bn being attributable to the public sector[1]. This figure in reality is likely to be significantly higher once other factors are taken into account. For example, the figure excludes several categories of losses reported in HMRC's tax gap estimate[2]. The estimate also does not consider losses due to error or to the various 'grey areas' between fraud and error, such as negligence and failure to take due care, and it only includes specific aspects of the shadow economy. Top-down econometric estimates of the shadow economy[3] suggest that tax losses and means-tested benefits overpayments may be considerably higher. Together these suggest that total detected and undetected losses for the broadest definition of fraud and error are likely to be significantly higher than the estimated £20.3bn. What is therefore clear is that the size of the problem is significant and that more needs to be done to combat fraud.

Current methods for sharing data, which involve establishing specific gateways for sharing specific data between specific parties through secondary legislation, are far too inflexible and slow to keep up with the constantly changing methods of fraud. Public authorities sometimes face delays of up to six years to understand the legislative landscape and then establish an appropriate gateway.

Rationale for intervention

Wider use of data sharing could improve the prevention, detection and investigation of fraud by:

a) aiding better targeting and risk-profiling of potentially fraudulent individuals;
b) saving taxpayers' money by streamlining processes; and
c) increasing the ability for Government to act more quickly on fraud and simplifying the legislative landscape.

There are clear calls to increase the effectiveness and/or the efficiency of current data sharing from across the public sector and some private sector organisations. The Law Commission scoping report, Data Sharing between Public Bodies[4], describes how the law surrounding data sharing is complex, with powers to share data scattered across a very large number of statutes. They may be set out expressly or implied. The report indicated that there are problems in practice and that there are differing interpretations of the law governing the sharing of data. In addition to the complex legal landscape, other issues include a reported lack of flexibility (the difficulty in adapting to changing circumstances in a timely fashion given legislative processes) and the time taken to create new data sharing relationships.

Policy objective

The policy intention is to reduce the likelihood and cost of fraud to the tax-payer by reducing the time and complexity involved in sharing data. We intend to do this by making it easier to allow parties to share data for the prevention, detection, investigation and prosecution of fraud, reducing the cost of accessing vital information necessary for combating fraud.

For example, two projects that would be enabled by a new power are Household Composition and the Single Fraud Investigation Service. The fraud recorded under Household Composition alone in 2014 was £650m, with losses expected to rise to £1.4bn in 2020. Sharing data would enable Departments to improve the detection and prevention fraud which could save over £300m.

Whilst the emphasis of any solution will be on flexibility, time and simplicity; it will be balanced by the need to protect the rights and privacy of individuals. Therefore we will ensure that principles of necessity and proportionality are understood and upheld.

Who the policy is meant to apply to

The policy is to make a general power that covers all public authorities and other bodies that carry out public functions by providing a service to a public authority. Organisations proposed to be included in the

schedule at introduction include Home Office, MoJ, HMRC, DoT, NHS Business Authority, Local Authorities in England and private bodies who fulfil a public function on behalf of a public authority. We anticipate posing the question in the proposed White Paper about whether the schedule should be extended to other organisations, which could usefully contribute to achieving policy objectives.

Description of Options considered

**Option 1: Do Nothing:** Allowing the creation of a number of specific statutory gateways, where there is a need for them.

This option is essentially maintaining the current status quo and making provision for each data-share required for the purposes of sharing data to combat fraud, through individual gateways widening existing statutory gateways or by creating new statutory relationships.

**Costs:** There would be a need to create specific legislation with each data sharing agreement. The cost associated with creating specific legal gateways is significant, in terms of Official, lawyer and Parliamentary time spent firstly in understanding the complex legal landscape, creating an appropriate gateway suitable for the specific needs and then passing the gateway through Parliament. The delay this creates in being able to identify and act on fraudulent activity also represents a cost whilst the gateway is being established.

**Benefits:** Specific gateways (created through secondary legislation) are least burdensome when it comes to producing evidence that such a gateway is required; in order to be added to statute it will be subject to Parliamentary scrutiny and therefore deemed necessary. To do so, it is expected that the case for each gateway will be clearly set out, providing assurance that such a measure was proportionate and necessary before it was created.

**Option 2: Providing for a broad, Government-wide presumption to share data;**

This option operates under the principle that data is an asset for the whole of Government. The proposal would essentially allow any public authority under the scope of this legislation to share any data for any purpose, so long as it was for the benefit of the public and was within the bounds of the Data Protection Act (DPA) and Human Rights Act (HRA).

**Costs:** There will be a transitional cost to Public Authorities in scope in terms of familiarisation with the new legislation, and potential training in how to provide the required information. We would also expect an ongoing cost related to the time spent gathering the required data together upon request. Specifically we would anticipate a higher amount of data sharing post legislation which would require more resources to service it by key data-holding organisations (e.g. DWP, HMRC) adding to the administrative burdens of departments as they service a higher demand.

Individual costs would accrue in terms of the possible impact on individual privacy and human rights. This would potentially lead to a reduction in trust, with possible consequences for health services, social care, policing and criminal justice amongst others and an increased likelihood of legal challenge (and therefore increased legal cost) based on the Human Rights Act.

**Benefits:** This option allows the most flexibility, shortest timescales for agreeing on a data share and will reduce legislative complexity the most.
The benefits are estimated from the collection of primary data from some departments. The figures do not represent a comprehensive assessment, merely the best estimate of the information we currently have available. Benefits comes from both the administrative cost savings, and anticipated reductions in fraud:

Administrative cost savings: Using internal Departmental surveys, which provides us with information on current and future cost and volume of data shares; we estimate the change in administrative costs due to the legislation to be in the region of a £0.25million saving based on the reduction of cost associated with each data share for a small number of departments.

There would also be an administrative saving from the reduction in the number of future data sharing agreements between Departments that would need to be set up individually compared with the hypothetical 'do nothing' scenario.

Overall, we would expect the net impact on Departments to be a net saving as increases in the volume of data sharing as a result of the legislation is expected by Departments to be outweighed by a reduction in the cost of sharing each element of data, and in setting up individual agreements.

Reduction in Fraud: Using information from HMRC on annual losses incurred due to fraud we have applied a purely hypothetical scenario where fraud was anticipated to have been reduced by 1%-5%. In this case, the benefit accrued is estimated to be £23-£115 million.[see table 1]

**These early indicative cost and benefit figures will be tested during the consultation and the final stage impact assessment will include a fuller assessment of the costs and benefits of each option.**

**Option 3: non-legislative work to change cultural boundaries: simpler guidance, brokerage of data-sharing agreements or other such provision (e.g. communities of practice);**
This option recognises the issue that a number of the barriers to effective data-sharing are cultural: overly-cautious interpretation of statute, trust in how other organisations will use data, incentives to withhold the supply of data, a lack of confidence in the integrity of the data being shared and a lack of consistent standards in definitions, formats and collection methodology. All these add to the issue of Departments being reluctant to share with each other and more broadly.

There is some work being carried out in this wider, cultural field. The Department of Communities and Local Government has established a 'Centre of Excellence' for data sharing across the Public Sector to share best practice and help overcome some of the cultural drivers that prevent data being shared.

**Costs:** There will be a cost in terms of creating, disseminating and training staff with the new guidance. However, this does not reduce *actual* legislative complexity, or the time taken, or the flexibility of any legislation of itself. As legislation would still be required, there would still be Parliamentary time and Administrative costs of setting up agreement when needed, as in the "do nothing" case.

**Benefits:**
This option would reduce *perceived* complexity of the legislation as clearer guidance is developed and best practice shared which will reduce *cultural* barriers to data sharing.

**Option 4: Constrained powers to share data for specific purposes within specified but flexible groups.**

In this area, the proposal is for constrained powers to share data for the specific purposes of prevention, detection, investigation and prosecution of fraud. It is envisaged that this power would have a scope that could permit a range of public authorities to take part.
The scope of this would be controlled by a prescribed list of organisations which would only be amended following an Order by a Minister. Details of the proposed solution are:

- To create a permissive legislative vehicle that allows a specific group of organisations to share any data for the prevention, detection, investigation and prosecution of fraud;
- To ensure that this facility is constrained:

  i. ensuring that organisations are only on the list if they can prove their need to be on it;
  ii. creating a Code of Practice that prescribed organisations must comply with in order to be able to maintain their prescribed status, this includes the publication of privacy impact assessments and auditing by the Information Commissioner and operating data sharing arrangements in alignment with DPA and HRA principles;
  iii. constraining the categories of information shared, in particular exempting non-relevant data classed as sensitive personal data for the DPA (race/ethnic origin, political opinions, religious beliefs or other similar beliefs, Trade Union membership, physical

or mental state or condition) and “patient information” as per the NHS Act s251(10); and

iv. preserving the unlawful disclosure sanctions of those organisations that have them - DWP and HMRC.

**Costs:** Costs are similar to those described in option 2. Although because this option has additional constraints on the power to share data, the individual cost in terms of the impacts on privacy and human rights is likely to be much lower.

As with option 2, there will be transitional costs to Public Authorities in scope in terms of familiarisation with the new legislation, and potential training in how to provide the required information. We would also expect an ongoing cost related to the time spent gathering the required data together upon request; a higher amount of data sharing would require more resources to service it by key data-holding organisations (e.g. DWP, HMRC) adding to the administrative burdens of departments as they service a higher demand.

**Benefits:** The benefits are similar to that outlined in option 2. There will be a benefit in terms of the reduction in fraud. If for example HMRC were to reduce the cost of fraud by 1%-5% as a result of the legislation, this would equate to a benefit of £23- £115 million (see table 1).

As with option 2, there will also be an administrative cost saving associated with not having to set up individual data sharing agreements between Departments compared with the hypothetical ‘do nothing’ scenario.

This option constrains the purposes for which data can be shared, and who can share that data. This option would therefore be less likely to reduce the public trust and confidence in Government’s ability to handle sensitive data: The constraints and safeguards would serve to reassure individuals that such a data-share would be done in a necessary and proportionate manner and that action would be taken should this not happen. Increasing the constraints will also serve to increase trust between organisations within the schedule, serving to reduce some of the cultural barriers to sharing data.

Finally, as legislation need not set out fully all categories of data being shared, it allows a greater agility when seeking to share changing categories of data. This, coupled with a more flexible set of parties that can share data for the purposes, will increase the likelihood of fraud activity being prevented helping to achieve the overall policy aim of a reduction in the cost of fraud.

Wider Impacts:
This option enables or provides an alternative route for a number of other policy initiatives such as the Counter Fraud Checking Service (CFCS).

**These indicative cost and benefit figures will be tested during the consultation and the final stage impact assessment will include a fuller assessment of the costs and benefits of each option.**

Risk and Assumptions

The proposed changes are intended to improve public sector bodies’ ability to investigate, detect and prevent fraud to reduce the likelihood and cost of fraud to the tax-payer by reducing the time and complexity involved in sharing data . The risks that these changes will bring about are common to any data sharing process, namely:

a) Loss of data;

b) Incorrect use of data – with biased or incorrect conclusions being drawn and policy ineffectively designed as a result;

c) Challenge from individuals whose data has been shared.

The use of data sharing has increased substantially in recent years and it is encouraged within Government to make better use of existing information. This has meant a better understanding of the risks associated with it. As a result, a number of measures have been developed to mitigate these risks. These mitigation measures are either required by law or considered as good practice and include among others:

- Organisations sharing data have the appropriate organisational measures in place as established by the Data Protection Act. It is good practice to:
  - design and organise security to fit the type of personal data disclosed or received and the harm that may result from a security breach
  - be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security
  - have an appropriate monitoring and auditing procedure in place
  - be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively
- Organisations sharing data have the appropriate technical measures in place as established by the Data Protection Act. It is good practice to:
  - make sure that the format of the data you share is compatible with the systems used by both organisations
  - check that the information that is shared is accurate before sharing it
  - establish ways for making sure inaccurate data is corrected by all the organisations holding it
  - agree common retention periods and deletion arrangements for the shared data
  - train staff so that they know who has the authority to share personal data, and in what circumstances this can take place.
- The various organisations involved in data sharing will each have their own responsibilities and liabilities in respect of the data they disclose or have received. It is therefore good practice:
  - for a senior, experienced person in each of the organisations involved in the sharing to take on overall responsibility for information governance, ensuring compliance with the law, and providing advice to staff faced with making decisions about data sharing
  - to have a data sharing agreement in place that includes:
    - The purpose of the sharing
    - The potential recipients or types of recipient and the circumstances in which they will have access
    - The data to be shared
    - Data quality – accuracy, relevance, usability, etc
    - Data security
    - Retention of shared data
    - Individual's rights – procedures for dealing with access requests, queries and complaints
    - Review of effectiveness/termination of the sharing agreement, and
    - Sanctions for failure to comply with the agreement or breaches by individual staff.

Overall, the appropriate mitigating measures depend on the type of information that is shared and the organisations that are sharing them. Therefore, any future policy that requires the use of data sharing should specify what mitigating measures are more appropriate to reduce risks.

Summary and Preferred Option:

**Option 1 (Do nothing option)** This has a number of drawbacks. It is essentially about maintaining the status quo of a network of specific data-sharing relationships; the creation of more would inevitably lead to a greater complexity in the overall architecture of data-sharing legislation, and not assist in speeding up the detection of fraud. Further, this option does not provide an inherent flexibility. Specific statutory gateways, particularly if they follow the current pattern, would not be able to accommodate the need for change of data-sharing in the area of fraud. The only way of accommodating this would be to keep creating new statutory gateways. This does not reduce the time it takes to create new relationships, nor does it seek to reduce complexity. On balance this option would not be the preferred option in this policy area.

**Option 2,** whilst providing the most flexible approach in terms of future-proofing data sharing, would also attract criticism for its broadness. This can be deduced from the reaction to the attempt at a similar, but slightly constrained, broad power set out under Clause 152 of the Coroner's and Justice Bill 2009. The clause failed to get through Parliament as it was deemed to have very little supporting evidence for such a large power, with very little constraint attached. A further argument, again employed on Clause 152 of the Coroners and Justice Bill, is that of its effect on the Data Protection Act and Human Rights Act. It is unlikely that such a presumption in favour of sharing data could be deemed to be proportionate in every case and could interfere with privacy. On balance this option would not be the preferred option in this policy area.

**Option 3** is necessary to facilitate data sharing and to promote a data sharing culture; this activity is already being taken forward by Government. However, this option is not sufficient, as it does not remove the legal barriers which limit the ability to share data.

**Option 4** provides the best approach to meeting the Government intention. Any such system would require governance around it as there will be decisions to be made about the ability of an organisation to share data, the necessity of that data to be shared for the prescribed purpose and the ongoing value of such a data-share. Given its ability to provide reduced complexity, greater flexibility and a degree of constraint that has not been attempted before, **this is the preferred option** that will meet the main challenge of this policy.

The proposals seek to create a permissive legislative vehicle that allows a specific group of organisations to share any data for the prevention, detection, investigation and pursuance of fraud. To ensure that this facility is constrained: ensuring that organisations are only on the list if they can prove their need to be on it; creating explicit reference to the DPA and HRA; and creating a specific need to uphold principles of proportionality and necessity when sharing data.

**Table 1: Benefits accrued from reduction of fraud (Scenarios for anticipated reduction of 1%, 3% and 5%)[5]**

| | | Current annual losses to your Department due to Fraud (£m) | Annual losses if reduced by 1% (£m) | Annual losses if reduced by 3% (£m) | Annual losses if reduced by 5% (£m) |
|---|---|---|---|---|---|
| **HMRC** | **Fraud** | 2,300 | 2,277 | 2,231 | 2,185 |
| | **Anticipated benefits accrued due to reduction in annual losses (£m)** | | 23 | 69 | 115 |

***Source: Departmental survey. These figures are indicative and do not represent a comprehensive assessment of the benefits associated with data sharing.***

[1] The most recent Annual Fraud Indicator (published March 2012 and found at: https://www.gov.uk/government/publications/annual-fraud-indicator) document sets the cost of Fraud and Error to the UK Economy as a whole as £73bn and provides a useful breakdown of this by sector.
[2] HM Revenue and Customs, Measuring tax gaps 2013 edition: Tax gap estimates for 2011-12, 11 October 2013
[3] Schneider, F. and Williams, C.C. (2013), The Shadow Economy, The Institute for Economic Affairs, London.
[4] http://lawcommission.justice.gov.uk/areas/data-sharing.htm

[5] These scenarios are purely hypothetical and not based upon any additional information