

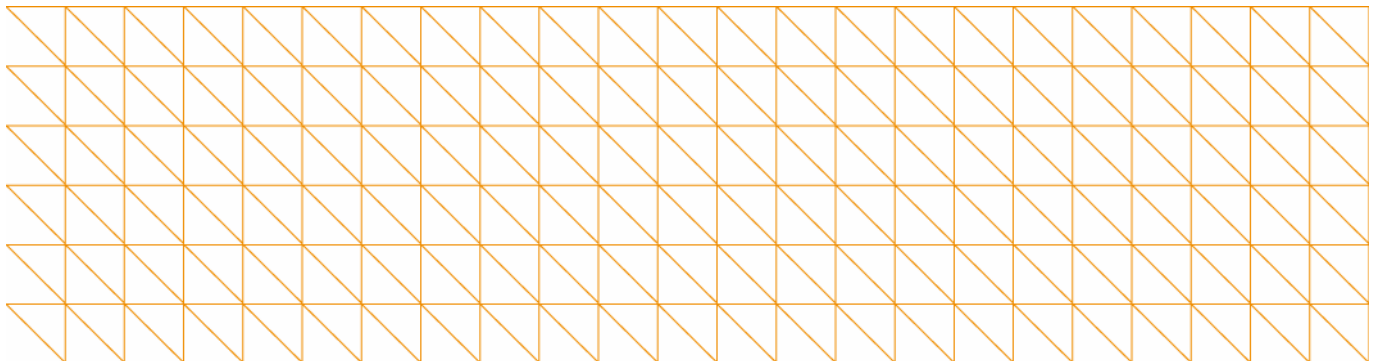


Ministry of  
**JUSTICE**

# Response to the Data Sharing Review Report

**Response to the Data Sharing Review Report**

24 November 2008





Ministry of  
**JUSTICE**

## **Response to the Data Sharing Review Report**

**Response to review carried out by Dr Mark Walport of the Wellcome Trust  
and the Information Commissioner, Richard Thomas**

**This information is also available on the Ministry of Justice website:  
[www.justice.gov.uk](http://www.justice.gov.uk)**

## Contents

Introduction and contact details	2
Background	3
Response to recommendations	4
Developing culture	6
The legal framework	14
The regulatory body	18
Research and statistical analysis	21
Safeguarding and protecting publicly available information	25
Conclusion and next steps	26

---

## **Introduction and contact details**

This document is the response to the Data Sharing Review Report. It will cover:

- background to the report
- a detailed response to the recommendations of the report, and
- the next steps following this document.

Further copies of this document can be obtained by contacting **Matthew Benson** at the address below:

**Matthew Benson**  
**Information Directorate, Ministry of Justice**  
**102 Petty France**  
**London**  
**SW1H 9AJ**

**Telephone: 020 3334 3769**  
**Email: [matthew.benson@justice.gsi.gov.uk](mailto:matthew.benson@justice.gsi.gov.uk)**

This document is available on the Ministry's website: [www.justice.gov.uk](http://www.justice.gov.uk)

## Background

On 25 October 2007 the Prime Minister asked Dr Mark Walport of the Wellcome Trust and the Information Commissioner, Richard Thomas, to independently review the framework for the use of personal information in the public and private sectors. The Review team issued a consultation on 12 December 2007 and conducted workshops to explore the issues raised in greater detail.

The terms of reference were to:

- consider whether changes were needed to the operation of the Data Protection Act 1998 (DPA);
- provide recommendations on the powers and sanctions available to the Information Commissioner's Officer (ICO) and the courts in the legislation governing data sharing and data protection; and
- provide recommendations on how data-sharing policy should be developed to ensure proper transparency, scrutiny and accountability.

The report was published on Friday 11 July and the recommendations focused on:

- cultural changes;
- changes to the legal framework;
- regulatory body changes;
- research and statistical analysis; and
- safeguarding and protecting personal information held in publicly available sources.

The Ministry of Justice published an initial response to the Review's report prior to the summer recess by written ministerial statement welcoming the publication.

Simultaneously the Ministry of Justice published its consultation paper, 'The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998'. This consultation was aimed at gathering views on some of the recommendations of the report and closed on 27 August 2008. To supplement the consultation, the Ministry hosted a workshop for stakeholders and interested parties to discuss issues relating to the ICO's powers and penalties in August 2008.

## **Response to recommendations**

The Government takes data protection seriously. Data protection safeguards are enshrined in the DPA and organisations are required to comply when processing personal data. Measures need to be taken to increase public trust and confidence in the handling and processing of personal data by both the public and private sectors. Following the publication of the Data Handling Review by the Cabinet Office and the Data Sharing Review by Richard Thomas and Dr Mark Walport, Government is implementing the key recommendations of these reviews to improve data management.

Government is keen to counter the common misconception that the DPA is always a bar to data sharing. The Data Sharing Review stated, 'The DPA is still commonly cited as a reason not to release information when it may be perfectly legitimate and in public interest to do so'. There is an appropriate balance that must be struck between the requirement to share data and the understanding that failure to share data also carries risks to vulnerable groups and individuals.

The sharing of personal data between Government departments in a secure and appropriate manner is essential to protect the public and to deliver public services. The ability of Government to share data performs a crucial role in, among other things, protecting children and other vulnerable groups and individuals; protects individuals against crime and disorder; and improves health and education provision.

The ability of Government to share data between departments is essential in providing and improving customer-focussed public service delivery and also ensures individuals get the services they require.

## Developing culture

### Recommendation 1

**As a matter of good practice, all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information.**

### Recommendation 2

**As a matter of best practice, companies should review at least annually their systems of internal controls over using and sharing personal information; and they should report to shareholders that they have done so.**

We agree with these recommendations, which complement the outcomes of the Cabinet Office 'Data Handling Procedures in Government: Final Report'<sup>1</sup> (DHR), published in June 2008. The DHR outlined the need for an increase in accountability and responsibility within Government departments and information management and risk must be sufficiently standardised to drive this. It also recognised the necessity to maintain a balance between avoiding bureaucracy within Government and the need to ensure important decisions are considered, recorded and implemented.

The DHR suggested the best mechanism to ensure this occurs was to put in place a chain of command from the Accounting Officer, with ultimate responsibility for ensuring appropriate controls are in place for their Department and an annual process of assessment. We agree with this and the other recommendations in the DHR for achieving compliance with the Data Sharing Review recommendations by Government departments.

Government departments have made significant progress implementing the requirements of the DHR. In particular, all Departments:

- have published information regarding data losses in their resource accounts for 2007/08 and will continue to do so on an annual basis;
- have appointed Senior Information Risk Officers (SIROs) with responsibility for the organisation's information risk policy, management and assessment; and

---

<sup>1</sup> [www.cabinetoffice.gov.uk/~media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625.pdf](http://www.cabinetoffice.gov.uk/~media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625.pdf).ashx

- are ensuring that those in their delivery chain, including public and private sector organisations, are aware of their responsibilities in relation to the new data handling measures.

The DHR stated Government departments would keep compliance with the recommendations of the DHR under annual review. This will be underpinned by the summary material in Government department's Statement on Internal Control, which are published annually and subject to peer review, through capability reviews when requested by Departments. In addition, Government departments resource accounts are subject to scrutiny by the Public Accounts Committee. External scrutiny of performance and capability will be provided through National Audit Office scrutiny of the Statement on Internal Control and spot checks by the Information Commissioner.

We support the recommendation and those organisations outside of the public sector should, if not already done so, clarify in their corporate governance or equivalent documents where ownership and accountability lies for the handling of personal information.

### **Recommendation 3**

**Organisations should take the following good-practice steps to increase transparency:**

**(a) Fair Processing Notices should be much more prominent in organisations' literature, both printed and online, and be written in plain English. The term 'Fair Processing Notice' is itself obscure and unhelpful, and we recommend that it is changed to 'Privacy Policy'.**

**(e) Organisations should use clear language when asking people to opt in or out of agreements to share their personal information by ticking boxes on forms.**

We agree that literature about data handling should be more prominent in organisations, not only in their literature but also in their culture. There are added benefits to organisations in ensuring their policies are written in plain English as their customers will be more inclined to share data with them, thereby potentially increasing revenues and repeat business.

We agree that the term 'Fair Processing Notice' could be seen by some as obscure and note that many organisations already use the term 'privacy policy'. However it must be for the organisations to determine the most appropriate terminology for their business area.

It is vital that opt-in and opt-out arrangements are clearly written and prominent so that people are clear about what they are agreeing to. The ICO is currently working on a code of practice on fair processing notices that will provide guidance to a wide range of organisations on best practice.

Government has shown its commitment to producing literature in plain English and many Government departments and Agencies have achieved the Plain English Crystal Clear Mark for their publications. The Crystal Mark is commonly seen as the standard that all organisations aim for when they produce public information. All documents including forms that achieve this standard must be clear to read, understandable and able to be acted upon by the intended audience.

**(b) Privacy Policies should state what personal information organisations hold, why they hold it, how they use it, who can access it, with whom they share it, and for how long they retain it.**

**(d) Organisations should publish and regularly update a list of those organisations with which they share, exchange, or to which they sell, personal information, including 'selected third parties'.**

We support these recommendations. All organisations should proactively publish details of their data sharing practices and schemes, in particular considering the criteria outlined in this recommendation. The DPA requires personal information to be processed fairly, and the ICO has the power to serve Enforcement Notices to compel a Data Controller to take specific steps to ensure they comply with legislation. Those who are obliged to register with the ICO already provide some of this information through the notification process and we will work with the ICO to make this process more efficient.

The DHR required Government departments to publish 'Information Charters'. The Information Charters set out the standards that people can expect from public bodies that request or hold personal data, how they can access personal data and what they can do if they do not think that these standards are being met. A sample Information Charter was provided for Government departments to use as a basis for their own charters.

There are circumstances, however, when it is appropriate not to publicise details of information held and how it may be shared, for example, in cases of national security, confidentiality agreements and market sensitivity. Where organisations are concerned about publication of this information, they should seek either professional legal advice as to whether or not it would be appropriate to do so in their particular circumstances.

**(c) Public bodies should publish and maintain details of their data-sharing practices and schemes, and should record their commitment to do this within the publication schemes that they are required to publish under the Freedom of Information Act 2000.**

We agree with the principle of this recommendation. Transparency should be an important consideration for all public bodies. Except where publication is inappropriate, we strongly encourage all public bodies to be transparent, proactively publishing details of their data sharing practices and schemes.

**(f) Organisations should do all they can (including making better use of technology) to enable people to inspect, correct and update their own information - whether online or otherwise.**

We agree with this recommendation. The government is committed to making better use of technology wherever appropriate to allow people to inspect, correct and update information held on them. We encourage all organisations to follow this recommendation, and consider that doing so is in the interest of any organisation that values accurate and up-to-date information.

It is important to note, however, in relation to recommendation 3 (a-f) that where the ICO feels an organisation's activity in any area concerning culture or good practice has resulted in that organisation contravening the DPA, then there are avenues currently available to the ICO to ensure organisations are brought into full compliance. The ICO can already request information from a data controller under an Information Notice to assist the ICO in assessing compliance with the DPA.

The ICO also has the potential for issuing an Enforcement Notice where it considers a data controller's activity may be contravening the DPA. When data controllers do not comply with these notices they are committing a criminal offence and the ICO is able to take appropriate action to force compliance with legislation.

We consider these current powers flexible and stringent enough for the ICO to regulate our data protection legislation effectively.

#### **Recommendation 4**

**All organisations routinely using and sharing personal information should review and enhance the training that they give to their staff on how they should handle such information.**

We agree with this recommendation. Training and awareness of good data security practice within Government departments was highlighted in the DHR. The core measures set out in the DHR included obligations for all Government departments to:

- have and execute plans to lead and foster a culture that values, protects and uses information for the public good, and monitor progress; and
- ensure that all data users must successfully undergo information risk awareness training on appointment and at least annually. In addition, all Information Assurance Officers (IAOs) must pass information management training on appointment and at least annually, and accounting officers, SIRO, and members of the audit committee must pass strategic information risk management training at least annually.

All Government departments are already addressing these core measures. The DHR stated that Government departments must complete initial programmes for providing data security training for all staff accessing protected personal data by October 2009 and set out the Government's plan to reform the overall arrangements within which departments manage information, through:

- core measures to protect information, including personal data, across Government to enhance consistency of protection and transparency of that protection to others;
- a culture that properly values, protects and uses data, both in the planning and delivery of public services;
- stronger accountability mechanisms, recognising that an individual department or agency is best placed to understand and address risks to their information, including personal data; and
- stronger scrutiny of performance, to build confidence and ensure those lessons are learned and shared.

As a result all Government departments have reviewed and improved training on data handling, or are in the process of doing so. A number of Departments have already developed training programmes for staff and these are underway, including Her Majesty's Revenue and Customs who are training around 90,000 staff. The NHS also launched a training programme on information risk in May, which will be available for over one million NHS staff. An e-learning training module is being developed by the Cabinet Office in conjunction with the National School for Government for use by all Government departments as well as the wider public sector including local Government and will be deployed in the autumn.

The Civil Contingencies Act 2004 places a statutory duty on certain organisations to share information in emergencies. Training should include arrangements for handling personal data in emergencies and form part of an organisation's contingency planning processes. All organisations need to have sensible plans in place for emergencies and their staff need to understand what they should do in an emergency. The Cabinet Office has released guidance to assist organisations in these instances, 'Data Protection and Sharing - Guidance for Emergency Planners and Responders, February 2007'.

In both the public and private sectors, staff should be trained to understand how to share information and deliver services in a way that protects personal data, and how to balance the risks of not sharing with the risks of doing so.

Organisations should regularly review and enhance training procedures, providing appropriate up-to-date training for staff involved with information handling, ensuring personal data is protected.

Should an organisation's activity in this area result in a contravention of the DPA, then the ICO will be able to use his regulatory powers as detailed under recommendation 3.

## **Recommendation 5**

**Organisations should wherever possible use authenticating credentials as a means of providing services and in doing so avoid collecting unnecessary personal information.**

We agree with this recommendation. The Government is committed to initiatives that streamline services and agrees that collecting unnecessary personal information should be avoided.

The Employee Authentication Service (EAS) is one Government initiative aimed at improving the delivery of public services. EAS is a scalable, sustainable and secure solution that enables employees in local government, schools and other organisations to access and share sensitive information in order to improve services for the benefit of children, learners and citizens.

EAS is currently being developed as a pan-Government service by the Department for Children, Schools and Families in partnership with the Department for Communities and Local Government, Department of Work and Pensions (DWP) and local authorities. EAS is being developed as part of Government Gateway, a DWP service that already provides online accounts to 13 million citizens and businesses for 152 Government services.

The service will provide common identity authentication that will:

- avoid the need for employees to go through multiple authentication processes and use multiple tokens (e.g. smart cards) every time they need to access sensitive information from different sources;
- support greater collaboration and joint working;
- provide alignment of processes and systems for sharing and accessing sensitive data in a secure way; and
- improve efficiency through re-use within central and local Government.

Tell Us Once is a major Government initiative looking at the feasibility of a service where citizens can report a birth, death or change of address to Government, only once ensuring Government responds in a co-ordinated manner. This would reduce the need for multiple contacts with Government over the same change in circumstances, thereby minimising identification processes that a citizen might usually need to go through. DWP is assessing the demand, costs and benefits of the service.

Tell Us Once is being tested through pilots involving Central Government and several local authorities, with different aspects of a potential service being trailed through various channels including face-to-face, telephone and online through the official Government website for citizens, Directgov.

We anticipate that Tell Us Once will not only result in fewer contacts for citizens, but will also promote more efficient Government services and a reduction in the personal information required by Government departments to deliver services.

In addition, the on-going work of the National Identity Scheme, which is an easy-to-use and extremely secure system of personal identification for adults living in the UK. The National Identity Scheme will prevent false or multiple identities being used by criminals or terrorists, but it will also protect individuals' identities and help them access services to which they are entitled.

A good illustrative example of authentication in the private sector is the process that many people go through in order to access services such as telephone or Internet banking, where Personal Identification Numbers (PIN) and other codes may be used rather than primary identification documents.

In order to remain viable, authentication schemes need to be continuously upgraded and updated. This process, in both the public and private sectors, should have the aim of ensuring they are robust enough to secure personal data while ensuring service provision is easily accessible to those that have the right to access it.

## **The legal framework**

### **Recommendation 6**

**Any changes to the EU Directive will eventually require changes to the UK's Data Protection Act. We recognise that this may still be some years away, but we nonetheless recommend strongly that the Government participates actively and constructively in current and prospective European Directive reviews, and assumes a leadership role in promoting reform of European data law.**

The Government is committed to ensuring that European data protection instruments continue to meet the high expectations of UK citizens, and will work to ensure that UK and European law remains properly equipped to deal with challenges brought by technological and social change.

We are aware of a number of current and prospective initiatives that have the aim of ensuring European data protection legislation remains fit for purpose in the long term. We are already engaging actively and constructively with these initiatives, particularly where they have the potential to impact on the DPA. Where shortcomings in the legal framework are identified, the Government will argue actively and constructively for necessary improvements. The European Commission last carried out an official review of the Data Protection Directive in 2007 and concluded the Directive lays down a framework that is 'substantially appropriate and technologically neutral'.

### **Recommendation 7(a)**

**New primary legislation will place a statutory duty on the Information Commissioner to publish (after consultation) and periodically update a data sharing code of practice. This should set the benchmark for guidance standards.**

The Government will bring forward primary legislation to place a statutory duty on the ICO to prepare, publish and review a code on the sharing of personal data (the Code). As part of this duty, the ICO will be committed to reviewing the Code, altering its provisions where appropriate. The Code will provide an excellent tool, assisting in ensuring public services operate to the highest standards, focussing on both the interests and needs of the public.

The two primary purposes of the Code will be to:

- provide practical guidance to the public, particularly data controllers and data processors, about how to share personal data in accordance with the requirements of the DPA; and
- promote good practice in the sharing of personal data.

There will be a definition of data sharing in the context of the Code. The definition will cover references to the disclosure of data by transmission, dissemination or otherwise making it available. The Code must be prepared and drafted in a manner consistent with the EU Directive as well as other international obligations.

A breach of, or compliance with, the Code will be taken into account by the courts, the Information Tribunal and the ICO whenever it is relevant to a question arising in legal or enforcement proceedings. This will ensure that the Code has an authoritative status. Compliance with the Code will, among other things, be taken into account in criminal proceedings relating to any offence under section 55 of the DPA. The Code will be admissible in evidence in any criminal or civil proceedings.

Before preparing or altering the Code, the ICO will be required to consult with trade associations and data subjects, or persons representing data subjects, as he considers appropriate.

Once the Secretary of State has confirmed that the Code or any alterations to it are compatible with the UK's national and international obligations, the Code or alterations will be placed before Parliament for approval.

### **Recommendation 7(b)**

**The new legislation should also provide for the Commissioner to endorse context-specific guidance that elaborates the general code in a consistent way.**

Government agrees that sector-specific codes should slot into the overall framework of regulation. The DPA<sup>2</sup> allows for the ICO endorsement of guidance. Where sector-specific guidance is required, the ICO should consult with business and those organisations that represent business in that sector to ensure the guidance is as useful and relevant as possible.

---

<sup>2</sup> Section 51(4) of the DPA provides for the Information Commissioner to encourage trade associations to prepare and disseminate codes of practice to their members. Where any trade association submits a code of practice to the Commissioner, the Commissioner may notify the association as to whether, in his opinion, the code promotes the following of good practice.

#### Recommendation 8(a)

**Where there is a genuine case for removing or modifying an existing legal barrier to data sharing, a new statutory fast-track procedure should be created. Primary legislation should provide the Secretary of State, in precisely defined circumstances, with a power by Order, subject to the affirmative resolution procedure in both Houses, to remove or modify any legal barrier to data sharing by:**

- **repealing or amending other primary legislation;**
- **changing any other rule of law (for example, the application of the common law of confidentiality to defined circumstances); or**
- **creating a new power to share information where that power is currently absent.**

#### Recommendation 8(b)

**Before the Secretary of State lays any draft Order before each House of Parliament, it should be necessary to obtain an opinion from the Information Commissioner as to the compatibility of the proposed sharing arrangement with data protection requirements.**

We agree with these recommendations. In the vast majority of cases, legislation itself does not provide a barrier to the sharing of personal data. The Data Sharing Review recognises the default position in the public sector has been to legislate, creating large numbers of specific legal gateways for sharing personal information. There are occasions when the requirement to share data should be put into primary legislation. Where this is evident, primary legislation should be sought as appropriate.

There will be times, however, when Government will seek to introduce data sharing arrangements as part of a package of measures to deliver a policy and a fast-track process would be more appropriate.

Government will legislate to create a gateway for data sharing powers, which will be subject to the Parliamentary Affirmative Resolution procedure. This will create a more streamlined process, retaining the element of parliamentary scrutiny to ensure transparency in data sharing policy and ensuring such power is proportionate. We intend to bring forward legislation to confer upon the Secretary of State a power to permit or require the sharing of personal information between particular persons or bodies, so long as a robust case can be made to use that power. The power will also be used to simplify the data protection framework and remove any unnecessary obstacles to data sharing.

The ICO should provide independent oversight of proposals being taken forward via this process. Proposals should also be subject to public scrutiny, followed by the mandatory publication of a Privacy Impact Assessment that describes the initiative and provides analysis on the proposal's implications for privacy and data protection, benefits for individuals and the general public.

## The regulatory body

### Recommendation 9

**The regulations under section 55A of the Data Protection Act setting out the maximum level of penalties should mirror the existing sanctions available to the Financial Services Authority, setting high, but proportionate, maxima related to turnover.**

The Ministry of Justice is working with the ICO to determine the level at which the maximum penalty should be set for serious breaches of the data protection principles which are likely to cause substantial damage or substantial distress to individuals. We can see the merits in using an existing established model and are considering the implementation of one similar to that operated by the Financial Services Authority.

### Recommendation 10

**The Government should bring the new fine provisions fully into force within six months of Royal Assent of the Criminal Justice & Immigration Act 2008, that is, by 8 November 2008.**

The new fine provisions<sup>3</sup> introduced in the Criminal Justice and Immigration Act 2008, but not yet commenced enable the ICO to impose monetary penalties on data controllers where there has been a breach. We are working with the ICO on these improvements and we hope to bring the new fine provisions into force shortly.

---

<sup>3</sup> Section 55A was inserted into the DPA by Section 144 of the Criminal Justice & Immigration Act 2008. It is not yet in force. On commencement of section 55A of the DPA, the Commissioner will be able to issue a civil monetary penalty for serious breaches of the data protection principles of a kind likely to cause substantial damage or distress. Section 55A will apply in cases of deliberate breach and where a data controller is aware that there is risk of serious breach but fails to take reasonable steps to prevent such a breach.

## Recommendation 11

**We believe that as a matter of good practice, organisations should notify the Information Commissioner when a significant data breach occurs. We do not propose this as a mandatory requirement, but in cases involving the likelihood of substantial damage or distress, we recommend the Commissioner should take into account any failure to notify when deciding what, if any, penalties to set for a data breach.**

We agree with this recommendation. As a matter of good practice any significant data breach should be brought to the attention of the ICO and that organisation should work with the ICO to ensure that remedial action is taken.

Following the publication of the DHR it is mandatory for Government departments to share details of significant actual or potential losses of personal data with the ICO. The ICO has already produced guidance for data controllers on when data breaches should be notified as a matter of good practice. The government is committed to the safe and secure handling of personal information and takes the loss of that information very seriously. We will give a mandate to the ICO to publish guidance for organisations on when to notify breaches of the data protection principles. The ICO will take into account the failure of an organisation to notify any breaches of the data protection principles when considering enforcement action.

In the Fourth Report of the House of Lord's Science and Technology Committee<sup>4</sup> the Government provided evidence to the Committee that recognised that the move towards breach notification legislation in other jurisdictions is an interesting development.

After considering the analysis of the experience of the United States in the area of data breach notification legislation the Government is not intending to implement similar legislation to that in operation in the US. By implementing the US system of mandatory breach notifications, we risk facing the same problems and mistakes that have occurred from the US experience. The recent paper by the Centre for Information Policy Leadership - 'Information Security Breaches - Thinking Back and Looking Ahead' – warns that the US approach to breach notification contributes little toward the security of personal data, with the framework being of 'diminishing utility over time'.

The Government is therefore committed to developing an approach that tackles the problems encountered in the US and is more suitable for the needs of robust data protection in the UK.

---

<sup>4</sup> <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16511.htm#a46>

### **Recommendation 12**

**The Information Commissioner should have a statutory power to gain entry to relevant premises to carry out an inspection, with a corresponding duty on the organisation to co-operate and supply any necessary information. Where entry or cooperation is refused, the Commissioner should be required to seek a court order.**

Our response to this recommendation is outlined in the package of measures set out in the response to the Ministry of Justice consultation on the Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998, published at the same time as this response.

### **Recommendation 13**

**Changes should be made to the notification fee through the introduction of a multi-tiered system to ensure that the regulator receives a significantly higher level of funding to carry out his statutory data-protection duties.**

Our response to this recommendation is outlined in the package of measures set out in the response to the Ministry of Justice consultation on the Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998, published at the same time as this response.

### **Recommendation 14**

**The regulatory body should be re-constituted as a multi-member Information Commission, to reinforce its status as a corporate body.**

We recognise the intention of this recommendation and will undertake further work to consider the case for reconstituting the Office of the Information Commissioner.

## **Research and statistical analysis**

### **Recommendation 15**

**'Safe havens' should be developed as an environment for population-based research and statistical analysis in which the risk of identifying individuals is minimised; and furthermore we recommend that a system of approving or accrediting researchers who meet the relevant criteria to work within those safe havens is established. We think that implementation of this recommendation will require legislation, following the precedent of the Statistics and Registration Service Act 2007. This will ensure that researchers working in 'safe havens' are bound by a strict code, preventing disclosure of any personally identifying information, and providing criminal sanctions in case of breach of confidentiality.**

### **Recommendation 16**

**Government departments and others wishing to develop, share and hold datasets for research and statistical purposes should work with academic and other partners to set up safe havens.**

We support these recommendations. Government is committed to handling data in accordance with the DHR, which put in place a set of guiding principles for putting the appropriate protections in place. Government recommends that individual sectors need to design approaches that are appropriate for their area of business within the general framework of data security already laid down by the DHR. A balance needs to be struck by any organisation between the importance of privacy and security with the need to drive forward essential research and analysis of performance data in the public interest.

The Office for National Statistics (ONS), the executive office of the UK Statistics Authority, and the Economics and Social Data Service (at the University of Essex) have systems in place for providing access to individual-level data for research and statistical purposes. ONS operates the Virtual Micro-data Laboratory (VML), an entirely self-contained and secure working environment where confidential individual data can be linked, matched, and analysed in all its detail by visiting researchers. The researchers and their projects are pre-approved. The only material that can leave the VML is statistical outputs that have been checked by ONS statisticians as being safe for publication. The VML is a safe haven for Approved Researchers.

The Economic and Social Data Service has begun the development of a remote access facility called the Secure Data Service (SDS). It shares many of the features of the VML. Pre-approved researchers can use purpose-built computer terminals to process data without holding a local copy of the information. The technology in the SDS ensures that the only copy of the data is held in the safety of the UK Data Archive, University of Essex. The SDS ensures that statistical results are checked for confidentiality risks, and sent to the researcher only when safe for publication. The SDS has different attributes to the VML, but is also a safe haven for approved researchers.

ONS hold a large amount of individual level data, for example about companies, from its business surveys and about individuals from economic and social surveys. It publishes statistics on its website that are aggregated and ensures that the statistics do not allow the reader to identify any individual or company. The individual-level databases are confidential. It is a criminal offence to disclose the individual level information held by ONS without lawful authority. However, a researcher can gain access to ONS' individual-level data with the approval of the National Statistician who has delegated decisions to the Microdata Release Panel (MRP) comprising a group of senior ONS officials.

A researcher wishing to access an individual-level dataset must apply to the MRP, giving detailed information about why the data is needed and the purposes for which it is to be used. The MRP will then consider whether there is lawful authority for the data to be disclosed and, if so, will decide whether it will approve the disclosure of the data to the researcher. If there is no existing legal gateway for the disclosure then ONS may invite the researcher to apply to be accredited as an 'Approved Researcher'. If successful, an Approved Researcher is granted temporary access to the individual-level dataset necessary for their research.

The data is very tightly controlled and is only disclosed if it is to be used for statistical/research purposes. There are conditions placed on the use of the data including the place where the data may be accessed and, if it is sent to the researcher, the importance of it being destroyed or returned to ONS on completion of its use for the declared purpose.

In relation to the Department of Health in England, we accept the recommendation that:

- 'safe havens' are developed, as an environment to assist with appropriate processing for the purpose of population-based medical research and statistical analysis for medical purposes, to minimise the risk of identifying individuals; and
- a system is devised to ensure that only accredited people do work within safe havens.

Through the Research Capability Programme, established via the NHS Connecting for Health in 2007 programme, the Department of Health is working with the Information Centre for Health and Social Care to develop safe havens. They will be designed to enable appropriate processing for health research purposes of patient information and other data derived from patient information.

The aim is to provide a secure environment in which suitable investigators and research professionals can work under conditions of confidentiality, with expert support from health professionals and staff who owe a duty of confidentiality equivalent to that of a health professional.

In this context, the Government will commission a code or codes for the use of safe havens, and a scheme for accrediting researchers. The Government will continue to consider the appropriate legal structures for the different types of processing that might in future be carried out using 'safe havens' and in relation to the use for non-medical purposes of data derived from patient information.

One aim of the Research Capability Programme is to determine principles to enable the use of information derived from care records alongside other datasets under conditions that protect identifiable personal and confidential information. The Department of Health will continue to work with Data Controllers and academic and other partners to achieve this, through safe havens where necessary.

### **Recommendation 17**

**The NHS should develop a system to allow approved researchers to work with healthcare providers to identify potential patients, who may then be approached to take part in clinical studies for which consent is needed.**

The Government has announced plans to ensure that patients, from every part of the country, with any illness or disease, are made aware of research that is of particular relevance to them; and to enable them to choose whether to take part in appropriate clinical trials.

The Department of Health will develop a system to allow approved researchers to work with healthcare providers for this purpose, under a duty of confidentiality equivalent to the duty owed by health professionals. The Department will develop mechanisms to help healthcare providers operate the system consistently, and will ensure they work with the employers of the approved staff to deal effectively with any breaches of confidentiality. The independent National Information Governance Board will monitor the operation of the system.

The Research Capability Programme in NHS Connecting for Health will develop secure ways to speed up the operation of the system and reduce the need for approved staff to process identifiable patient information.

In relation to the NHS in England, the draft NHS Constitution includes pledges about access to information and informed choice. The Handbook to the draft NHS Constitution explains how these pledges will apply to research, stating:

*Research is a core part of the NHS because it enables the NHS to improve the current and future health of the population. Therefore, the NHS will do all it can to give patients, from every part of the country, with any illness or disease, a right to know about research that is of particular relevance to them and, if they choose, to take part in approved medical research that is appropriate for them. Patients can therefore expect that a health professional or a research professional who owes the same duty of confidentiality as a health professional may use care records, in confidence, to identify whether they are suitable to participate in approved clinical trials. Appropriate patients will be notified of opportunities to join in, and will be free to choose whether they wish to do so, after a full explanation.<sup>5</sup>*

In relation to the research that it supports through the National Institute for Health Research (NIHR) in England, the Government will:

- require NHS research sites to display standard notices drawing attention to the way personal information may be used for research;
- ask the National Information Governance Board<sup>6</sup> to amend the NHS Care Record Guarantee so that it draws appropriate attention to the use of personal information for research and analysis to improve health and care;
- ensure wide distribution of the NHS Care Record Guarantee when revised;
- require NHS organisations to publish their research Privacy Policies, research data-sharing practices, and lists of the organisations with which they share personal information for purposes related to research;
- prepare standard explanatory material on research uses of personal information, making it publicly available through NHS Choices, and available to NHS research sites for local use; and
- develop better mechanisms to record individual patients' objections to research uses of information that identifies them, in a way that enables any NHS research site to respect their wishes.

---

<sup>5</sup> Handbook to the draft NHS Constitution, June 2008, page 24

<sup>6</sup> The Health and Social Care Act 2008 amended Section 250 of the National Health Service Act 2006, establishing an independent National Information Governance Board for Health and Social Care

## **Safeguarding and protecting publicly available information**

### **Recommendation 18**

**The Government should commission a specific enquiry into on-line services that aggregate personal information, considering their scope, their implications and their regulation.**

We consider that this recommendation may merit further consideration. In relation to identity theft, we must take into account the extent to which such services provide a sufficient source of information to facilitate fraudulent activity. To date there has been no overall assessment of this and we encourage any initiatives that seek to reduce the availability of personal information that could lead to identity fraud.

However we acknowledge the complexity of issues involved in undertaking this type of enquiry. For example, the source of personal details used to commit an identity fraud is usually not known, and there may be more cost-effective ways to reduce identity theft.

### **Recommendation 19**

**The Government should remove the provision allowing the sale of the edited electoral register. The edited register would therefore no longer serve any purpose and so should be abolished. This would not affect the sale of the full register to political parties or to credit reference agencies.**

Regulations introduced in 2002 govern the sale of the edited register and allow an elector to opt out, protecting their details from being supplied to a third party if they wish. We are aware that opt out rates vary significantly across the UK with rates in some areas being as low as 20% and others in the region of 70%.

Before committing to any course of action we need to establish how removing the provisions would impact not just on individuals but the economy as a whole. We therefore propose to conduct a public consultation on this recommendation. This will enable us to build a firmer evidence base about the advantages and disadvantages of the edited register and consider the way forward on the basis of the responses to the consultation.

## **Conclusion and next steps**

Government is continuing to put in place the appropriate structures and procedures to take account of the DHR.

Where indicated above, we will work closely with the ICO to ensure any further work on these recommendations is done so in order to protect people's personal data more effectively by both the public and private sectors.

We have previously signalled our intentions in May 2008 to bring forward changes in the draft legislative programme under the area of strengthening data protection laws through the audit powers of the ICO<sup>7</sup>. Proposals requiring secondary legislative change will be brought as and when appropriate to do so.

---

<sup>7</sup> House of Commons draft legislative programme 2008-09

© Crown copyright  
Produced by the Ministry of Justice