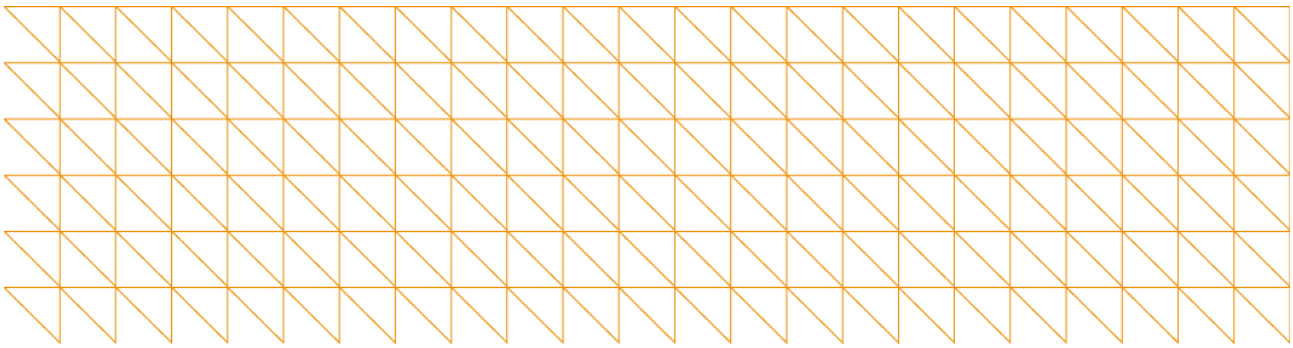
Ministry of Justice

Assessment Notices under the Data Protection Act 1998

Extension of the Information Commissioner's Powers

Response to Consultation CP9/2013

This response is published on 15 July 2014



Ministry
of Justice

Assessment Notices

Extension of the Information Commissioner's Powers

Response to consultation carried out by the Ministry of Justice.

This information is also available on the Ministry of Justice website: www.justice.gov.uk

About this consultation

To:	NHS data controllers across the United Kingdom
Duration:	From 25/03/13 to 17/05/13
Enquiries (including requests for the paper in an alternative format) to:	Bilal Toure Information and Devolution Policy Ministry of Justice 102 Petty France London SW1H 9AJ Telephone: 020 3334 5028 Email: dataprotection@justice.gsi.gov.uk

Contents

Introduction and contact details	3
Background	4
Summary of responses	6
Responses to specific questions	7
Conclusion and next steps	10
The consultation criteria	13
Annex A – List of respondents	14

Introduction and contact details

This document is the post-consultation report for the consultation paper, Assessment Notices under the Data Protection Act 1998, Extension of the Information Commissioner's Powers.

It will cover:

- the background to the report
- a summary of the responses to the report
- a detailed response to the specific questions raised in the report
- the next steps following this consultation.

Further copies of this report and the consultation paper can be obtained by contacting **Bilal Toure** at the address below:

Information and Devolution Policy
Ministry of Justice
102 Petty France
London SW1H 9AJ

Telephone: 020 3334 5028
Email: dataprotection@justice.gsi.gov.uk

This report is also available on the Ministry's website: www.justice.gov.uk.

Background

The consultation paper *'Assessment Notices under the Data Protection Act 1998, Extension of the Information Commissioner's Powers'* was published on 25 March 2013. It invited comments on the proposal to designate NHS bodies in the UK for the purposes of the Information Commissioner's powers to serve assessment notices.

In 2011, the Information Commissioner (ICO) submitted a business case to the Ministry of Justice, recommending that the Secretary of State use his order making powers under section 41A (2) (b) of the Data Protection Act 1998 (DPA) to extend the powers of the ICO to carry out compulsory assessments of public authority NHS bodies compliance with data protection principles under the Act. The evidence provided in the business case demonstrated that the NHS was an area within which the use of assessment notices would be beneficial. The ICO's powers of compulsory audit already extend to government departments[1].

Before making an order of this kind, the Secretary of State must consult the ICO (section 67(3), DPA). Apart from consulting the ICO, there are no other statutory requirements to consult more widely, although the Government felt it important to informally consult with NHS bodies to understand the impact of the proposal in the context of the ongoing structural reforms within the NHS.

The main factors upon which the ICO based his recommendations were:

- The sector processes large amounts of sensitive personal data;
- The ICO receives a high number of complaints and self-reported breaches of the DPA by NHS bodies;
- The ICO's Good Practice team have identified many examples of significant risks to individuals' personal data in its consensual audits of the NHS;
- The number of consensual audits of NHS bodies (53%) is significantly below the average across the public sector as a whole (71%).

The designation of NHS bodies would require them, in response to a request from the ICO, to among other things: permit the ICO to enter the organisation's premises; direct him to documents of a specified description; assist him to view information using equipment on the premises; and permit him to observe the processing of any personal data which takes place on the premises.

In the consultation paper the Government proposed that, in light of recommendations from the ICO alongside the evidence presented in his business case, NHS bodies in England, Wales, Scotland and Northern Ireland should be designated under section 41A (2) (b) of the Data Protection Act 1998 (DPA). This would give the ICO powers to serve any NHS

[1] Government departments are covered under section 41A(a) whilst other public authorities must be designated under section 41A(b)

body with an assessment notice to enable him to establish whether that NHS body has complied or is complying with the data protection principles under the DPA.

As outlined in his *Assessment Notice code of practice*[2], the Information Commissioner sees auditing as a constructive process with real benefits for data controllers and data subjects alike and so aims to establish, wherever possible, a participative approach. In doing so he has indicated that his power to serve an assessment notice is very much a backstop and that his preference is for organisations to volunteer for consensual audits in the first instance unless the circumstances make this inappropriate.

The consultation period closed on 17 May 2013 and this report summarises the responses, including how the consultation process influenced the proposal consulted upon.

A list of respondents is at **Annex A**.

[2] www.ico.org.uk/~/.../**assessment_notices_code_of_practice**_2012.ashx

Summary of responses

1. A total of 76 responses to the consultation paper were received. Of these, 58% were from NHS bodies. Responses were also received from members of the public (23%), the private sector (9%), the Third sector (4%), local authorities (3%), professional bodies and trade associations (3%).

2. The responses were analysed for possible new approaches to data protection compliance; evidence of the impact of the proposal; levels of support and any key observations from both those who agreed with and those who disagreed with the proposal.

3. The table below provides a breakdown of the responses received in terms of overall numbers and percentages, with particular focus on NHS bodies.

	Proposal
Yes	67 (88% of total responses) (93% of NHS bodies)
No	9 (12% of total responses) (6% of NHS bodies)

Responses to specific questions

Do you agree that the Information Commissioner should be given powers under the Data Protection Act 1998 to carry out non-consensual assessments of data of NHS bodies for compliance with the Act?

The majority of responses received were in favour of extending the powers of the Information Commissioner to carry out compulsory audits of NHS bodies' compliance with the DPA. Respondents generally viewed the extension of powers as sensible and proportionate. Many provided helpful suggestions and input about how they could be best implemented in practice.

The most commonly held view was that extending the ICO's powers of compulsory audit would lead to an increase in the uptake of consensual audits by NHS bodies. This would enable the ICO to identify areas of risk in terms of data protection compliance and to work with NHS bodies to mitigate these to prevent serious incidents occurring. This is in line with the ICO's preferred method of practice and is seen as the most effective way of improving the handling of personal data.

There was a general acknowledgment that there had been a number of cases where breaches had occurred and the ability to take formal action by way of a compulsory audit was therefore a necessary tool for the ICO to have. In addition, respondents recognised that the ICO saw the powers of compulsory audit as a backstop to be used only when absolutely necessary and welcomed the ICO's overriding commitment to provide advice, support, and expert knowledge and guidance to assist organisations in achieving compliance.

Those respondents not in support of extending the Information Commissioner's powers were generally opposed on the basis that it would place additional burdens on an already heavily regulated sector. The following quote is representative of a number of these respondents: "NHS Trusts are currently subject to regulation regarding the use of personal data. This regulation includes the mandatory completion of the Information Governance Toolkit, which requires the Trust to score against 42 requirements which cover compliance with the Data Protection Act, confidentiality and information security. NHS Trusts are further regulated by the Care Quality Commission Essential standards, some of which relate to the use of patient data. To introduce compulsory audit by the Information Commissioner in addition to this would cause duplication of work and would not be an efficient use of the time of staff responsible for this area".

Another respondent thought a more balanced approach was needed, with action being taken to raise reporting levels amongst private sector organisations. Other respondents highlighted the fact that an increasing number of NHS services are being delivered by private sector providers but that they were not included in the scope of the proposal to extend the Information Commissioner's powers.

Response to concerns about the impact of the proposal.

Whilst the majority of respondents supported the proposal in principle, a number sought clarity on how the proposals would work in practice and reassurance that the proposals would not place additional burdens on NHS bodies.

The main concerns are outlined in the table below with added commentary from the ICO.

Issue	**ICO Response**
How often will an NHS Body get audited by the ICO using the new powers?	When identified on a risk assessment basis.
The scope of the proposed audit consists of five areas. In practice would the audit just focus on the areas on which the NHS Body had received complaints e.g. Subject Access Requests?	No. Usually 3 scope areas are undertaken and these are agreed with the data controller as far as possible; however the ICO will take into account any relevant information e.g. complaints.
Can you provide reassurance that unannounced visits will not cause disruption?	Visits are not unannounced. Compulsory audits are only conducted when a data controller has failed to respond to a request for a consensual audit or has refused consent without adequate reason. The ICO try to conduct as much of the audit offsite, such as review of policies and limit time on site to a maximum of 3 days. (See the ICO Assessment Notices Code of Practice[3])
How does the ICO intend to evaluate the effectiveness of the new powers, if granted?	The power is a tool to support the ICO's risk based audit programme. The ICO will always look to conduct a consensual audit in the first instance and will weigh up the effectiveness of the power each time it is used.
The proposed compulsory audits have the potential for being too onerous. Why can't they be combined with Care Quality	The ICO is working closely with the Health and Social Care Information Centre in the development of the IG Toolkit to ensure that there is minimal

[3] http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/audits

Commission audit or the Information Governance toolkit?	duplication. The ICO have recently accepted a place as observer on the CQC National Information Governance Committee and we will continue to review its processes in light of engagement with all interested stakeholders.
Will the compulsory audits be informed/guided by the existing criteria on the Information Governance (IG) Toolkit? Will the compulsory audits be informed/guided by the existing Outcome 21 in the Care Quality Commission Standards? Will they be informed/guided by relevant standards in the NHS Litigation Authority requirement e.g. around health records?	The ICO has its own control framework and the auditors are familiar with the IG toolkit. The ICO are aware of the CQC Essential Standards and will continue to review our own procedures to ensure they are consistent The ICO will continue to engage with internal and external stakeholders to ensure its work is proportionate and appropriately considers controls which are widely considered to be important in delivering compliance with the DPA 1998.
Will compulsory audits have clear guidelines with defined standards? Will there be a "score" that we are required to achieve?	There will be an overall assurance rating of compliance with DPA. This is detailed in the Assessment Notices Code of Practice.
What will the status of the IG Toolkit be if the audit is introduced? Will Trusts still be required to do the toolkit?	It will still be a requirement to complete the IG Toolkit.
What is Monitor's role in this? Are they being consulted? Will they be setting standards based on this new ICO audit?	We will continue to consider the results of Monitor Risk Assessments when prioritising our work.

Conclusion and next steps

1. Based on the evidence presented by the Information Commissioner in his business case and the responses from NHS bodies and others to the consultation document, the Government believes a compelling case has been made for extending the ICO's powers of compulsory audit to public authority NHS bodies. The Government believes the benefits include:

    a. Encouraging NHS bodies to improve their compliance with the data protection framework.

    b. Incentivising NHS data controllers to sign up to consensual audits.

    c. Improving public confidence in regards to the protection of sensitive personal data by NHS bodies.

2. As set out in his *Assessment notices code of practice*, the Information Commissioner sees the compulsory audit power as a strong driver in persuading data controllers to sign up to a consensual audit. The power itself is not designed to investigate individual breaches of the DPA but rather to review the processes, policies and procedures of NHS bodies to ensure compliance with the DPA's principles.

Scope of the new powers

3. The range of public authority NHS bodies to which we will extend the power of compulsory audit will reflect the "traditional" public sector providers of NHS services listed in Schedule 1 part III of the Freedom of Information Act 2000, and Schedule 1 part 4 of the Freedom of Information (Scotland) Act 2002. In practical terms, this will entail designating in an order, bodies such as Foundation Trusts, GP Practices, Clinical commissioning groups but not contracted private and third party sector companies providing NHS services such as pharmacies, opticians and dentists. In addition, the Health and Social Care Information Centre (HSCIC), established under the Health and Social Care Act 2012, with powers to collect information, including identifiable and confidential information, about the health care that people receive, will also be designated.

4. The Government will continue to work closely with the Information Commissioner to ensure he has adequate powers to enforce compliance with the DPA by organisations that handle personal data. This includes keeping under review whether it might be appropriate at some point in the future to make an order under S41A (2) (c) of the DPA which would extend the ICO's powers of compulsory audit to private and third sector contractors of NHS services. It is important to note however that all providers of NHS Services, including private and third sector providers, are covered by the DPA and have to comply with the data protection principles when handling personal data.

5. The designation will be undertaken by way of secondary legislation via a Statutory Instrument. We anticipate the designation order will come into force by the end of the year. We will work with the Department for Health and devolved

administrations to ensure that the proposal is applied to all relevant public authority NHS bodies consistently across the UK. The designation order itself will be reviewed within 5 years to consider whether it remains appropriate for the bodies to remain designated.

Consultation Co-ordinator contact details

If you have any comments about the way this consultation was conducted you should contact Sheila Morson on 020 3334 4498, or email her at: sheila.morson@justice.gsi.gov.uk.

Alternatively, you may wish to write to the address below:

Ministry of Justice
Consultation Co-ordinator
Better Regulation Unit
Analytical Services
7th Floor, 7:02
102 Petty France
London SW1H 9AJ

The consultation criteria

The seven consultation criteria are as follows:

1. **When to consult** – Formal consultations should take place at a stage where there is scope to influence the policy outcome.

2. **Duration of consultation exercises** – Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

3. **Clarity of scope and impact** – Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

4. **Accessibility of consultation exercises** – Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.

5. **The burden of consultation** – Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

6. **Responsiveness of consultation exercises** – Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

7. **Capacity to consult** – Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

These criteria must be reproduced within all consultation documents.

Annex A – List of respondents

Community and Acute Foundation NHS Trust

Health and Social Care Board for Northern Ireland

Cwm Taf Health Board

NHS Protect

Salem Health Project

Leeds and York Partnership NHS Foundation Trust

FairWarning UK Limited

Public Health Wales

Royal College of Nursing

South West Yorkshire Partnership Foundation Trust

Western Health and Social Care Trust

Luton Borough Council

Northumbrian Water

Birmingham Community Healthcare NHS Trust

Leeds Community Healthcare NHS Trust

Blackpool Teaching Hospitals

Risk Factory

Kaleidoscope Consultants Limited

NHS Shared Business Services

Association for the Improvement of Maternity Services

Health and Social Care in Northern Ireland

Care UK LTD

Kent and Medway Commissioning Support Unit

Brighton and Sussex University Hospitals NHS Trust

Northern Ireland Social Care Council

Peterborough & Stamford Hospitals NHS Foundation Trust

NHS Wales

National Aids Trust

Mid Yorkshire Hospitals NHS Trust

North Yorkshire & Humber Commissioning Support Unit

South Tees Hospitals NHS Foundation Trust

Kent and Medway Commissioning Support Service

Amberhawk Training Ltd

Essex Council

North East Ambulance Service

Acute NHS Foundation Trust

eCulture Solutions

Royal Orthopaedic NHS Hospital Foundation Trust

Sheffield Teaching Hospitals NHS Foundation Trust

Leeds and York Partnership NHS Foundation Trust

South West London and St. George's Mental Health NHS Trust

South Warwickshire NHS Foundation Trust

Yorkshire Ambulance Services NHS Trust

South Eastern Health & Social Care Trust

NHS Greater Glasgow and Clyde

London Ambulance Service Trust Ltd NHS

Birmingham Children's Hospital NHS Foundation Trust

NHS Redditch and Bromsgrove Clinical Commissioning Group

NHS Wyre Forest Clinical Commissioning Group

NHS National Services Scotland

Camera Watch

South Tees Hospitals NHS Foundation Trust

Coventry and Warwickshire NHS Partnership NHS Trust

Birmingham and Solihull NHS Trust

Kent and Medway NHS and Social Care Partnership Trust

British Medical Association

PharmacyVoice Ltd

Big Brother Watch

We also received 18 responses from members of the public.