



Ministry of
JUSTICE

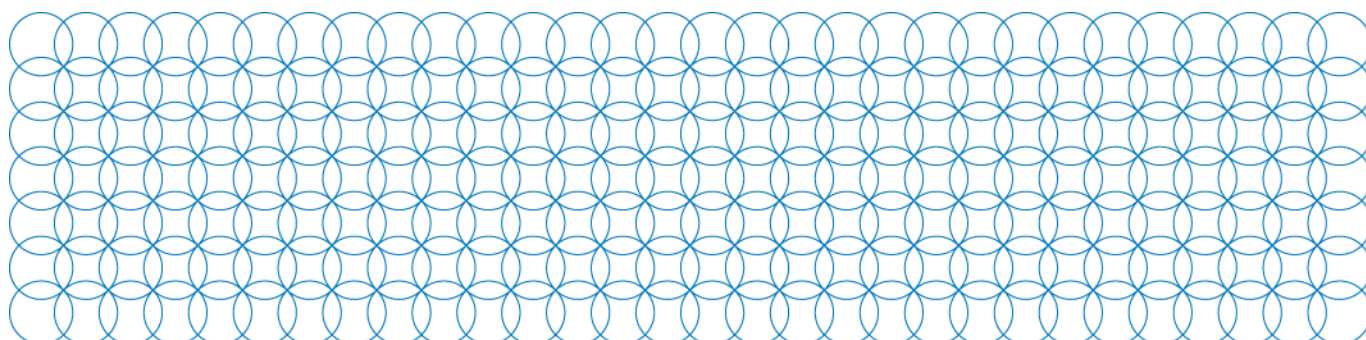
Assessment Notices under the Data Protection Act 1998

Extension of the Information Commissioner's Powers

Consultation Paper **CP9/2013**

This consultation begins on 25 March 2013

This consultation ends on 17 May 2013





Ministry of
JUSTICE

Assessment Notices

Extension of the Information Commissioner's
Powers

**A consultation produced by the Ministry of Justice. It is also available on the
Ministry of Justice website at www.justice.gov.uk**

About this consultation

- To:** This consultation is aimed at NHS data controllers in England, Wales and Northern Ireland bodies and Health Service data controllers in Scotland
- Duration:** From 25/03/13 to 17/05/13
- Enquiries (including requests for the paper in an alternative format) to:** Michael Anima-Shaun
Ministry of Justice
102 Petty France
London SW1H 9AJ
Tel: 020 3334 3189
Email: michael.animashaun@justice.gsi.gov.uk
- How to respond:** Please send your response by 27 May 2013 to:
Michael Anima-Shaun
Ministry of Justice
102 Petty France
London SW1H 9AJ
Tel: 020 3334 3189
Email: dataprotection@justice.gsi.gov.uk
- Response paper:** A response to this consultation exercise is due to be published within 3 months of the close of this consultation paper at: <http://www.justice.gov.uk>

Contents

Introduction	3
The proposals	6
Summary	20
Questionnaire	21
About you	22
Contact details/How to respond	23
Consultation principles	25
Annex 1 – Named Consultees	26

Introduction



The NHS is one of the largest data controllers in the UK, processing a huge amount of sensitive personal data on a daily basis. It is therefore important for confidence in the NHS that the public feel reassured that their personal data is being handled in compliance with the Data Protection Act and personal data losses and other breaches that can result in considerable harm and distress are avoided.

The Information Commissioner has requested that the Secretary of State use the Order-making power under section 41A (2)(b) DPA to extend the powers of the Information Commissioner to carry out compulsory assessments of NHS bodies' compliance with the data protection principles under the DPA.

In support of this proposal the Information Commissioner has provided evidence, by way of a business case, which forms the basis of this consultation, and which demonstrates that the NHS is an area within which the use of the assessment notice power would be beneficial and targets all NHS data controllers in England, Wales and Northern Ireland and Health Service data controllers in Scotland.


The Information Commissioner's Office (ICO) already has the power to assess the following of good practice by NHS bodies, entering with their consent, under Section 51(7) of the DPA. The proposal to move from consensual to non-consensual assessment powers is informed by the ICO's experience working with NHS bodies to improve their compliance with data protection law and favours a more preventative approach to increasing compliance within the sector.

The designation of NHS bodies would involve no new obligations beyond their existing obligations to comply with the DPA and to that end the Information Commissioner has agreed to work closely with the Care Quality Commission to agree a Memorandum of Understanding to avoid duplication of burden on NHS bodies, ensuring a collaborative approach and providing for the sharing of knowledge and intelligence.

For the most part, this consultation follows the Consultation Principles issued by the Cabinet Office. However, given that this is a sector specific targeted consultation we consider that a reduced consultation period of 8 weeks rather than 12 is appropriate in this instance.

An Impact Assessment has not been completed for this proposal as impact is limited to the public sector and the costs involved are likely to be below £5m per annum.

I look forward to receiving your responses.

A handwritten signature in black ink, appearing to read 'Tom McNally', written in a cursive style.

Lord McNally
Minister of State for Justice

The proposals

1. The Government proposes that, in light of recommendation from the Information Commissioner, public authority data controllers within National Health Service Bodies (NHS) in England, Wales, Scotland and Northern Ireland are designated under section 41A (2) (b) of the Data Protection Act 1998 (DPA) meaning that they would be liable to be subject to compulsory data protection audits.

Assessment notices

2. 'Assessment notices', under section 41A of the DPA, are for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles. Government departments are covered by section 41A (2) (b). Other public authorities must be designated by an order made by the Secretary of State.
3. An assessment notice is a notice which can require a data controller to do any of the following:
 - (a) permit the Information Commissioner to enter any specified premises;
 - (b) direct the Information Commissioner to any documents on the premises that are of a specified description;
 - (c) assist the Information Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises;
 - (d) comply with any request from the Information Commissioner for—
 - (i) a copy of any of the documents to which the Information Commissioner is directed;
 - (ii) a copy (in such form as may be requested) of any of the information which the Information Commissioner is assisted to view;
 - (e) direct the Information Commissioner to any equipment or other material on the premises which is of a specified description;
 - (f) permit the Information Commissioner to inspect or examine any of the documents, information, equipment or material to which the Information Commissioner is directed or which the Information Commissioner is assisted to view;
 - (g) permit the Information Commissioner to observe the processing of any personal data that takes place on the premises;
 - (h) make available for interview by the Information Commissioner a specified number of persons of a specified description who process personal data on behalf of the data controller (or such number as are willing to be interviewed).

4. As required by section 41C of the DPA, the Information Commissioner has prepared and issued a Code of Practice to address how his functions in connection with assessment notices will be exercised. This Code is available on the Information Commissioner's Office (ICO) website.

Data protection compliance in the NHS

5. NHS Bodies process huge quantities of, often sensitive, personal data. Most individuals will have no choice but to interact at some point with their hospital or GP. It is therefore particularly important that the public have the assurance that this information being processed in compliance with the DPA.
6. The evidence compiled by the ICO through complaints from the public, data security breach reports, investigations and audits conducted with consent, demonstrates that significant compliance problems exist within the NHS.
7. The Information Commissioner has a range of options to apply effective sanctions against those who have already breached the DPA. The ability to serve an assessment notice provides the opportunity to identify and mitigate risks *before* a breach occurs. It also provides the opportunity where a problem has been identified to step in, identify specific weaknesses in systems and procedures, and provide and follow up practical advice to resolve the problems.
8. The Government's modernisation of the NHS, which also affects local government, will be implemented over the next few years. In the NHS, Strategic Health Authorities and Primary Care Trusts will be replaced by Clinical commissioning groups (CCGs) from April 2013. These CCGs will become responsible for commissioning most healthcare – planning, buying and monitoring services to meet the needs of their local communities. The Government's reforms also place Directors of Public Health within local authorities which the Government believes will drive health improvements in a more holistic and innovative way.
9. As these reforms bed in, and organisational responsibilities change and personal data is transferred, every effort should be made to ensure data protection risks do not increase. These risks may be particularly acute over the next few years but the underlying problems are not short-term issues. The long-term ability to conduct compulsory audits (subject to review every 5 years) would allow the Information Commissioner to intervene if there are significant concerns, see what is happening in practice and provide practical recommendations to mitigate identified risks.

Complaints to the Information Commissioner's Office

10. Over the last six years health has been in the top sector areas where the Information Commissioner has received complaints of potential data protection breaches from individuals.

Complaints by sector and financial year

Complaints	2007	2008	2009	2010	2011	2012	Total
Lenders	7,355	1,989	3,873	1,960	1,696	2,119	18,992
Local Government	598	664	937	1,213	1,146	1,389	5,947
General business	557	657	867	998	1,191	1,115	5,385
Health	517	722	833	1,036	1,040	1,167	5,315
Central Government	696	754	766	815	689	736	4,456
Policing and criminal records	685	624	728	797	490	564	3,888
Telecoms	594	530	704	594	507	531	3,460
Debt collectors	290	295	402	374	336	275	1,972
Education	241	242	318	427	390	501	2,119
Insurance	183	202	245	347	349	304	1,630
Internet	179	218	259	339	254	298	1,547
Retail	193	183	215	223	265	287	1,366
Other	117	179	280	309	147	554	1,586
Solicitors /Barristers	112	96	192	286	210	258	1,154
Housing	83	102	167	236	197	243	1,028
Utilities	112	130	148	150	138		678

Figure 1: Total data protection complaints received by the Information Commissioner by sector and year – Top 15

11. The complaints received and upheld by the Information Commissioner from members of the public (Figure 2) demonstrate that the compliance problems in the health sector covers a wide range of issues.

12. The most common basis for upheld complaints (a case where the Information Commissioner has concluded it was unlikely the organisation complied with the principles of the DPA in a specific situation) in the health sector¹ is a failure to comply with an individual's right of access to their information followed by breaches of security and inappropriate/unauthorised disclosures of data.

	Health
Subject access	1,234
Disclosure of data	242
Security	225
Inaccurate data	82
Fair processing info not provided	19
Right to prevent processing	14
Use of data	8
Obtaining data	9
Excessive/Irrelevant data	4
Retention of data	5
Section 55 (criminal offence)	9
Notification	2
Total	1,454

Figure 2: Upheld data protection complaints to the Information Commissioner - breakdown by nature - 2007 to date

13. In addition to the issues identified through individual complaints the Information Commissioner receives reports of security breaches directly from organisations themselves. Although there is no statutory requirement for the NHS to report data protection breaches, NHS in England are required to report certain more serious security breaches to the ICO². Other organisations may decide to voluntarily report breaches.

¹ Our case management system records cases under the sector 'health' rather than the 'NHS'. Figures will include a small number of complaints about private sector healthcare providers but the vast majority of cases will relate to processing by organisations within the NHS.

² <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igap/dnletter20may08.pdf>

Sector	Disclosed in Error	Lost Data/Hardware	Lost in Transit	Non-secure Disposal	Stolen Data/Hardware	Technical/Procedural Failure	Other	Total
Central Gov	31	47	13		18	19	1	129
Local Gov	158	54	7	6	96	41	19	381
NHS	113	156	22	23	169	45	24	552
Other	19	9	1		16	4	4	53
Other Public	80	38	11	2	52	17	13	213
Private	184	99	22	15	177	88	35	620
Third Sector	12	14	1		22	6	3	58
Telecoms	3	2			1	2	1	9
Grand Total	600	419	77	46	551	222	100	2015

Figure 3: Self reported breaches 2007 to date by sector and nature of breach

14. The majority of problems reported directly to the Information Commissioner (Figure 3) relate to security issues such as loss or theft of personal data. The range of concerns identified indicates procedural and human failures across a range of different areas. The root cause of such a variety of problems can be difficult to address without the opportunity to see in practice how policies and procedures are being applied and followed on the ground.

Sector	Breach type	
NHS	Disclosed in Error	15
	Lost Data/Hardware	14
	Lost in Transit	1
	Non-secure Disposal	2
	Other	4
	Stolen Data/Hardware	7
	Technical/Procedural Failure	4
Total		47

Figure 4: Breakdown of NHS self reported breaches in the last quarter

15. Examples of specific breaches reported by NHS recently have included:

- A Urology operating diary containing a summary of 147 patient's information lost from a secure office area.
- Mammography Screening Forms of over 50 women which contain names, addresses, dates of birth, NHS Numbers and GP details left on a train.

- Documents including clinical information relating to 147 patients found on the ground outside a hospital. The majority of the patients were identified on operating lists.
- Two boxes containing approximately 200 dental records dating back to the 1980s found in a shed in the grounds of a closed down clinic.
- Two unencrypted data sticks with data of approximately 1800 patients lost.
- Three faxes for individual patients containing sensitive personal data were sent on three different dates to the wrong person.
- Unencrypted memory stick found in the street outside a hospital. The stick contains information about some hundreds of renal patients and included their name, medical records number and in some cases the home address, date of birth and telephone number.

Taking action – addressing data protection breaches

16. In the majority of individual cases where a breach of the DPA is likely to have occurred the Information Commissioner will resolve the complaint by recommending remedial action to the data controller. Where more formal measures are necessary the range of options available to change the behaviour of organisations breaching the rules includes obtaining undertakings, serving enforcement notices and issuing civil monetary penalties.
17. The Information Commissioner has used the powers available to him to try to improve compliance across the NHS. This has included obtaining numerous undertakings committing data controllers in the NHS to improve compliance. Recent undertakings have included:
 - **South London Healthcare NHS Trust** - Undertaking to comply with the seventh data protection principle following the loss of two unencrypted memory sticks, the leaving of a clipboard with ward lists attached in a grocery store and a failure to adequately secure some patient paper files when not in use. 11 April 2012
 - **University Hospitals Coventry & Warwickshire NHS Trust** - Undertaking to comply with the seventh data protection principle following two separate incidents involving the loss of personal data by the Trust including details of medical procedures and test results being found in a bin by a member of the public - 27 October 2011
 - **Dartford and Gravesham NHS Trust** - Undertaking to comply with the seventh principle following the accidental destruction of 10,000 archived records. The records – which should have been kept in a dedicated storage area –were put in a disposal room due to lack of space - 4 October 2011

18. Monetary penalty notices are reserved for the most serious and negligent data protection breaches. Recent notices have included:
- A monetary penalty notice of £225,000 served on **Belfast Health and Social Care Trust** following a serious breach of the Data Protection Act. The breach led to the sensitive personal data of thousands of patients and staff being compromised. The Trust also failed to report the incident to the ICO.
 - A monetary penalty notice for £325,000 served on **Brighton and Sussex University Hospitals NHS Trust** following the discovery of highly sensitive personal data belonging to tens of thousands of patients and staff – including some relating to HIV and Genito Urinary Medicine patients – on hard drives sold on an Internet auction site in October and November 2010. June 2012
 - A monetary penalty notice for £90,000 served on **Central London Community Healthcare NHS Trust (CLCH)** for a serious contravention of the DPA, which occurred when sensitive personal data was faxed to an incorrect and unidentified number. The contravention was repeated on 45 occasions over a number of weeks and compromised 59 data subjects' personal data. May 2012. The notice was appealed to the First-tier Tribunal (Information Rights) and the Commissioner's notice was upheld by the Tribunal (January 2013).
 - A monetary penalty of £70,000 issued to the **Aneurin Bevan Health Board** following an incident where a sensitive report - containing explicit details relating to a patient's health - was sent to the wrong person. April 2012.
 - A monetary penalty of £175,000 served on **Torbay Care Trust** following an incident where information relating to over a thousand staff was published on the Trust's website. This included names, dates of birth and National Insurance number. August 2012.
 - A monetary penalty of £60,000 issued to **St George's Healthcare NHS Trust** after a vulnerable individual's highly sensitive medical details were sent to the wrong address. The data subject had not resided at the address for nearly five years. July 2012.
19. These cases clearly illustrate the problems that are occurring. Taking formal action when a breach happens is an effective and important mechanism for ensuring data controllers take compliance seriously and take steps to prevent issues recurring. It would however clearly be ideal for risk areas to be identified and practices to be improved across an organisation long before such serious incidents occur.

Identifying risks and achieving compliance - the value of the audit process

20. Obtaining evidence and assurances from organisations through written submissions and reviewing policies and procedures is an important mechanism for the Information Commissioner to understand the way organisations work and to provide advice on the measures they have put in place to comply with the DPA. However, relying on written assurances from organisations and reviewing procedures clearly has limitations. The Information Commissioner's experience of conducting audits has provided real evidence of the value of the audit process in identifying problem areas and assisting organisations in implementing real world, practical solutions that meet their needs.
21. Many of the recommendations resulting from the audit process are ones which could only have been identified through an on-site visit. These include identifying sensitive medical files left in areas clearly visible and accessible to the public and computers left logged into systems containing sensitive personal data in public areas. Audits have also identified lapses in physical security measures such as a lack of visitor procedures, files with personal information left in unlocked storage left open to the public and confidential waste inappropriately disposed of.
22. While, in the Assessment notices code of practice, the Information Commissioner has given assurances that the audit process is not aimed at identifying opportunities for enforcement, some of the findings of audits in these sectors have identified the sorts of concerns that, in some cases, may have led to enforcement action if discovered in the course of investigating a breach or from a self reported breach.
23. The Information Commissioner recognises that organisations will often conduct their own self assessment and internal audits of processes, for example the NHS Information Governance Toolkit. Whilst any work in this area is worthwhile, an audit by the Information Commissioner provides independent, specialist expertise and allows for dissemination of standards and good practice across organisations.
24. It is not anticipated that NHS organisations will be excessively burdened by the audits. They are designed to minimise the impact on day to day operations and, where consent has been given, the timing of the audit will always be agreed with the organisation, taking into account factors such as operational pressures, resource availability and organisational change. For consensual audits, all timings are agreed up front in a Letter of Engagement and realistic timescales set for the different stages of the audit process. In particular, the time on site completing fieldwork at organisation is limited in the majority of cases to three working days, and a schedule of interviews is agreed beforehand to minimise the impact on business.

25. In addition, the scope of a consensual audit, including locations and departments to be covered, are agreed in advance with organisations, taking into account the organisation’s preferences, as well as risk factors and other assurance work, such as internal audits and other independent verification. The audits are specifically designed to focus on the areas of greatest risk, while limiting the disruption to the provision of services.

Consensual audits

26. The Information Commissioner’s Good Practice team have conducted a number of consensual of audits of NHS organisations. These audits have in many cases been prompted by particular concerns.

	NHS		
	Red	Amber	Yellow
2009/10		2	
2010/11		3	3
2011/12		1	4
Total		6	7

Figure 5: Number of consensual audits conducted by the Information Commissioner by year with grading – NHS³

27. The audits conducted by the Good Practice team have identified some common themes for risks across the NHS. Many of these are examples of significant risks to individual’s personal data that would be very difficult to identify without conducting an audit.

28. It is also worth noting that audits also identify areas of good practice, and having a team of independent auditors working across these sectors allows for the sharing of examples of how to efficiently and effectively meet DPA obligations amongst organisations. Examples of good practice are always identified in our audit reports and, wherever possible, recommendations take into account policies and procedures which we have seen working in practice in other organisations.

³ Gradings were not provided for audits prior to 2009/10

The NHS

29. Security of personal data in practice is particularly difficult to assess without the ability to audit an organisation. This is especially the case for manual data which is still in regular use in the NHS.

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
Green	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
Yellow	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.
Amber	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. There is therefore a real risk that the objective of data protection compliance will not be achieved. Actions to improve the adequacy and effectiveness of data protection governance and control have been agreed and timetabled.
Red	No assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide no assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

Figure 6: Audit overall assurance opinion grading criteria

30. In a number of NHS organisations audited by the Information Commissioner, security of manual data was graded a significant risk. Specific problems identified included lockable storage not being used, patient records left in reception trays openly accessible and insecure confidential waste bins.
31. Other issues that have been highlighted through audits of NHS data controllers include unencrypted mobile media holding sensitive personal data, weaknesses in training, lack of monitoring of compliance and lack of practical application of records management policies.
32. **Case study 1** – Problems identified in this audit of an NHS Hospital Trust included; data protection policies overdue for renewal, training pass rate reported at 95% but more detailed reports indicate in some areas of the Trust the pass rate was significantly lower than average – particularly among medical staff, equipment observed lying in corridors, spot checks on compliance should be carried out but no evidence these checks were being undertaken, not everyone wearing ID badges, policy required no storage of personal data on portable media but this doesn't work in practice because no controls or assurance that staff are complying with the policies, no evidence of regular review of access privileges for shared folders and systems, policy required monitoring of systems on a regular basis but did not happen in practice because it is resource intensive, passwords routinely set/ re-set without presentation of ID, procedures on leavers were not effective meaning that immediate access removal could not be guaranteed.
33. **Case study 2:** The audit was carried out following amalgamation of several health boards. Specific problems identified included; No routine security checks on the activities of data processors after a contract was signed, 'mandatory' training on the DPA had in reality not been completed by the majority of staff, portable media remained unencrypted, no local monitoring of subject access requests to ensure compliance in practice.
34. **Case study 3:** Several personal data losses from the Trust prompted the audit. Specific problems identified included; intranet linked to outdated or inaccurate policies and procedures, the information asset framework did not include manual personal data at all, the clear desk policy to prevent patients seeing sensitive personal data is not monitored, only 80% of laptops were encrypted, staff responding to subject access requests did not have sufficient training.
35. **Case study 4:** The theft of unencrypted information prompted the audit. Problems identified included; policies on DP did not cover subject access rights, significant inconsistencies in the training received by different types of staff - more advanced training for those who need it was not provided, long standing staff have not received induction training at all and there was no robust process for ensuring refresher training is provided (only 542 out of 4000 staff had passed the training module), staff working directly with patients had limited awareness of access rights, records in outpatient and inpatient areas were left unattended on open trolleys and desks that could be accessed by anyone, password complexity in practice was not in line

with Trust's own user guide (6 chances to guess password and then after lock out user can try again), 30 minutes of inactivity before screens lock out, staff using the same password for access to the network and all applications, home working taking place without risk assessment (in contravention of policies) because the responsible post was vacant, no pro-active monitoring of access and use of the main patient management system (no record of browsing, printing or data export), no figures of records going missing to monitor frequency and nature of incidents.

Follow up

36. Areas of concern identified in an audit will be highlighted to the data controller and specific recommendations made about how to resolve the problem. These recommendations will be followed up in a number of ways. The Information Commissioner focuses on the areas of greatest risk and will pursue these areas up with specific requests for evidence that recommendations have been addressed and a further visit if required.
37. In 2010/11 the 11 follow up audits conducted showed that 92% of the Information Commissioner's recommendations were either fully or partially implemented by organisations. Particularly considering the issues identified in audit may well be long standing problems that an organisation has struggled to address in the past this figure clearly demonstrates that the recommendations are taken seriously and that this process is an effective mechanism for ensuring compliance.
38. Dependent on the progress made, the Information Commissioner revises its audit opinion when completing its follow up audit report to recognise the actions taken by organisations to mitigate the identified risks. In May 2011, the Information Commissioner started to publish these follow up audit reports in order to allow organisations to demonstrate the progress they have made. When the Information Commissioner returns to complete these audits, nearly 70% of organisations have an improved audit opinion.
39. The audit report is provided to staff at a senior level within the organisation who will commit to the recommendations, timescales for compliance and individual ownership of actions. This ensures senior staff have a clear awareness of any problems highlighted and are directly engaged with the process of resolving those problems.

Agreeing to an audit

40. Although organisations can and do ask to be audited in some cases many of the consensual audits conducted have only come about because a problem has already occurred and the Information Commissioner been able to exert some pressure on the organisation to agree to the process. On 5 September 2011 Christopher Graham and Sir David Nicholson sent a

joint letter⁴ to the Chief Executives of all Strategic Health Authorities, Chief Executives of NHS Trusts and Chief Executives of all Primary Care Trusts calling their attention to the ability of the Information Commissioner to carry out a data protection audit and encouraging organisations (particularly those newly providing NHS services) to accept.

41. Most audits that have already been conducted in the NHS have come about as referrals from the Information Commissioner's Enforcement team. Even in this situation, where a serious data protection problem has occurred, and has been exposed, organisations can still be reluctant to agree to an audit. Of the NHS organisations referred for audit by Enforcement only 53% have ultimately committed to an audit.
42. This compares to 71% across the public sector as a whole. In particular, the response to letters to police forces and probation trusts (67% and 56% respectively agreeing to an audit) has been particularly encouraging.
43. Where the power to serve an assessment notice exists data controllers can agree to consensual audits without the notice being necessary in each case. The Information Commissioner has not had to serve an assessment notice to date because 100% of data controllers covered by the existing provisions have agreed to an audit (knowing the option to serve a notice exists if they refuse). The figures above do however demonstrate clearly that without that power to back up requests for access organisations will continue to be reluctant to volunteer. Those data controllers that have something to hide, particularly those who know their processes and controls are insufficient, are perhaps the most likely to want to avoid or postpone closer inspection.

Scope of the ability to conduct compulsory audits

44. The Information Commissioner proposes that the designation of NHS data controllers in England, Wales and Northern Ireland refers to the designation of National Health Service Bodies in the Freedom of Information Act 2000 schedule 1 Part III, anticipating that this will be amended following the NHS reforms in England. He additionally proposes that the definition for the Health Service data controllers in Scotland refers to the relevant sections in the definition in schedule 1 Part 4 of the Freedom of Information (Scotland) Act 2002.
45. The Information Commissioner is aware that the public would reasonably expect that all providers of NHS services should be subject to compulsory audit. However, he accepts the complexity of current NHS structural reforms, particularly in England and that adding private and third sector providers would require an additional order under section 41A(2)(c). He will therefore gather further evidence to support the case for an additional order, at a later date.

⁴ http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_129895.pdf

46. Outside the scope of this business case on 41A(2) the Commissioner is keen to explore the extent to which contracts with NHS service providers could specify an obligation on providers to agree to an ICO audit, if they are not designated under section 41A(2)(b).
47. The Information Commissioner is aware of the requirement on the Care Quality Commission (under the Health and Social Care Act 2012) to drive improvements in information governance across the NHS. The Commissioner is working closely with the Care Quality Commission to agree a Memorandum of Understanding to avoid duplication of burden on public health organisations, to ensure a collaborative approach and to provide for the sharing of knowledge and intelligence.

Resource for conducting audits

48. The introduction of the higher tier fee for notification has enabled the Information Commissioner to be confident he can resource this additional audit activity. The Information Commissioner's Good Practice team is already set up to carry out this work with staff in place holding audit and data protection qualifications.
49. The Information Commissioner takes a risk based approach to all audit activities to ensure these resources are focused on the areas of greatest need. The Information Commissioner recognises the pressures on individual organisations and the audit process is designed to have as limited an impact as possible on the day to day operations of the data controller.

Summary

50. The evidence set out above clearly demonstrates that the NHS is an area where there are already significant and widespread data protection compliance concerns. Data controllers in these sectors are managing huge quantities of complex and often sensitive personal data, they are often involved in wide scale data sharing initiatives and engaging multiple data processors. The nature of the personal data held by these organisations is such that a breach of the DPA often has particular potential to cause real distress and harm.
51. These problems are already evident and, as set out above, the pressures on organisations in these sectors are only likely to increase in the next few years. The NHS in particular is entering a period of huge restructure which will involve responsibility for sensitive personal data shifting to completely new bodies.
52. The Information Commissioner already invests significant time and effort providing advice and guidance to those trying to comply. He can and does use the powers available to him to take action against organisations that breach the rules. In these sectors in particular the ability to compel data controllers to allow the Information Commissioner to audit their practices is an essential tool to identify and mitigate risks before serious problems occur. As set out above simply relying on organisations agreeing to an audit is not sufficient. A power of compulsion is needed even if in practice this serves mainly as an incentive to organisations to sign up to a consensual audit. The value of the audit process is clearly illustrated and the extension of the assessment notice power will provide a clear basis for the Information Commissioner to improve data protection compliance in these areas of significant risk.

Questionnaire

We would welcome responses to the following question:

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?

Thank you for participating in this consultation exercise.

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	
Date	
Company name/organisation (if applicable):	
Address	
Postcode	
If you would like us to acknowledge receipt of your response, please tick this box	<input type="checkbox"/> (please tick box)
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

Contact details/How to respond

Please send your response by 17 May 2013 to:

Michael Anima-Shaun
Ministry of Justice
Information Rights and Devolution
6th Floor, Post Point 6:17
102 Petty France
London SW1H 9AJ

Tel: 0203 334 3189

Email: dataprotection@justice.gsi.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Ministry of Justice at the above address.

Extra copies

Further paper copies of this consultation can be obtained from this address and it is also available on-line at <http://www.justice.gov.uk/index.htm>.

Alternative format versions of this publication can be requested from [email/telephone number of sponsoring policy division].

Publication of response

A paper summarising the responses to this consultation will be published in [insert publication date, which as far as possible should be within three months of the closing date of the consultation] months time. The response paper will be available on-line at <http://www.justice.gov.uk/index.htm>.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that

confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Consultation principles

The principles that Government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles.

<http://www.cabinetoffice.gov.uk/sites/default/files/resources/Consultation-Principles.pdf>

Annex 1 – Named Consultees

NHS Chief Executives and Chairs (including Foundation Trust Chief Executives and Chairs in England and Wales)

NHS bodies and organisations in England and Wales

NHS bodies and organisations in Scotland

HSC bodies and organisations in Northern Ireland

GP Practice Managers

Monitor Chief Executive

The Care Quality Commission

© Crown copyright 2013
Produced by the Ministry of Justice

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Alternative format versions of this report are available on request from 0203 334 3189 or dataprotection@justice.gsi.gov.uk