

Business case for the extension of Assessment Notice powers

Introduction

This document sets out the Information Commissioner's recommendation to the Secretary of the State that data controllers within the National Health Service (NHS) and local government are designated under section 41A (2)(b) of the Data Protection Act 1998 (the DPA).

Under section 41A the Information Commissioner may serve designated data controllers with a notice (an 'assessment notice') imposing specific requirements on the data controller. The 'assessment notice' is for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles. This process is referred to in the Information Commissioner's Code of Practice¹ as a 'compulsory' audit.

Government departments are covered by section 41A (2) (b). Other public authorities must be designated by an order made by the Secretary of State.

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—

¹ Assessment Notices Code of Practice
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/~media/documents/library/Corporate/Detailled_specialist_guides/ASSESSMENT_NOTICES_CODE_OF_PRACTICE.ashx

- (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).

The evidence set out in this document demonstrates that in the two areas where the Information Commissioner would like to be able to use the assessment notice power - the NHS and local government – there are particularly significant and widespread data protection compliance concerns. The success of having this power in practice has been clearly illustrated by the fact that the Information Commissioner has not had to serve an assessment notice to date. 100% of those central government data controllers currently covered who have been asked to agree to a consensual audit have done so.

Indeed it is important to note the Commissioner sees the extension of his powers as backstop, albeit a necessary one, in the areas of the NHS and local government. He expects that it will be only rarely that he has to go so far as to serve a formal assessment notice. However his experience with central government tells him that the existence of a compulsory audit power is a strong driver in persuading data controllers to sign up to a consensual audit.

This case sets out the recommendation for the specific designation of data controllers within the NHS and local government. There are other areas, in the

public and private sector, where data controllers process huge volumes of personal data and evidence demonstrates significant compliance problems exist. The ability to serve an assessment notice (and therefore undertake compulsory audits) is a very powerful tool for the Information Commissioner to identify data protection risk and ensure measures are put in place to mitigate those risks before real harm occurs in any sector. Going forward, where the evidence supports the case, the Information Commissioner will recommend the extension of the assessment notice power in other areas. He is already collecting evidence and developing a case to support an extension to some categories of data controllers in the private sector. In the meantime he will continue identifying problem areas, promoting the benefits of consensual audits and monitoring take up across the public and private sector.

Data protection compliance in the NHS and Local Government

Both the NHS and local government process huge quantities of, often sensitive, personal data. Most individuals will have no choice but to interact at some point with their local council, hospital or GP. It is therefore particularly important that the public have the assurance that this information being processed in compliance with the DPA.

The evidence compiled by the Information Commissioner's Office (ICO) through complaints from the public, data security breach reports, investigations and audits conducted with consent, demonstrates that in areas of both the NHS and local government significant compliance problems exist.

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.

The next few years are likely to be a time of particularly significant upheaval for the NHS and local government. The NHS in particular is looking at complete reorganisation. This will include the dismantling of Strategic Health Authorities and Primary Care Trusts to be replaced by Clinical Commissioning Boards. Responsibility for public health initiatives (and in some cases treatment of individuals) is to be passed from the NHS to local authorities. Local government's involvement with the third sector and outsourcing of services also looks set to continue.

This reorganisation, huge transfers of personal data and potential confusion over responsibilities, has the potential to create more significant data protection risk. These risks are likely to 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 where 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

Over the last 5 years local government and health have 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

	2007	2008	2009	2010	2011	Total
Local Government	598	664	937	1,213	698	4,110
General business	557	657	867	998	623	3,702
Health	517	722	833	1,036	593	3,701
Central Government	696	754	766	815	430	3,461
Policing and criminal records	685	624	728	797	241	3,075
Telecoms	594	530	704	594	267	2,689
Debt collectors	290	295	402	374	216	1,577
Education	241	242	318	427	209	1,437
Insurance	183	202	245	347	215	1,192
Internet	179	218	259	339	139	1,134
Retail	193	183	215	223	175	989
Other	117	179	280	309	78	963
Solicitors /Barristers	112	96	192	286	120	806
Housing	83	102	167	236	115	703
Utilities	112	130	148	150	85	625

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

The complaints received and upheld by the Information Commissioner from members of the public (Figure 2) demonstrate that the compliance problems in

these two sectors cover a wide range of issues. 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 both the health sector² and local government 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	Local Government
Subject access	816	1,001
Disclosure of data	142	332
Security	174	114
Inaccurate data	57	49
Fair processing info not provided	14	40
Right to prevent processing	12	12
Use of data	5	10
Obtaining data	3	12
Excessive/Irrelevant data	3	10
Retention of data	3	7
Section 55 (criminal offence)	6	1
Notification	2	
Total	1,237	1,589

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

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 either the NHS or local government to report data protection breaches, NHS in England are required to report certain more serious security breaches to the ICO³. Other organisations may decide to voluntarily report breaches.

² 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.

³ <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

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

Examples of specific breaches reported by local government and NHS over the last six months have included:

- The personal data of 1822 staff was accidentally shared via e-mail to a clinical reference group.
- A Urology operating diary containing a summary of 147 patients 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.
- A spreadsheet containing personal details of 200 housing waiting list customers emailed in error to just over 150 recipients. These recipients included partner agencies, carers and a number of individuals.
- 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

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 behavior of organisations breaching the rules includes obtaining undertakings, serving enforcement notices and issuing civil monetary penalties.

The Information Commissioner has used the powers available to him to try to improve compliance across the NHS and local government. This has included obtaining numerous undertakings committing data controllers in the NHS and local government to improve compliance. Recent undertakings have included:

- **Rochdale Metropolitan Borough Council** - Undertaking to comply with the seventh data protection principle following an incident in which an unencrypted USB stick containing personal data relating to thousands of local residents was lost - 3 November 2011
- **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
- **Dumfries and Galloway Council** – Undertaking to comply with the seventh principle of the DPA following the accidental online disclosure of current and former employee’s personal data in response to a Freedom of Information (Scotland) Act request - 17 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

- **Walsall Council** – Undertaking to comply with the seventh principle following the accidental disposal of postal vote statements in a skip by the council’s data processor. The council did not have a written agreement with the data processor selected to store this personal data - 9 September 2011
- **London Borough of Greenwich** – Undertaking to comply with the seventh principle of the DPA following two incidents where sensitive personal data was inadvertently disclosed, due to the Council's failure to implement appropriate wording in their ICT policy, stating that the sending of sensitive personal data in business related emails to external webmail addresses should be avoided. 10 August 2011
- **Lewisham Council** - Undertaking to comply with the seventh data protection following the discovery of an unencrypted USB stick containing thousands of tenant records and financial data in a London pub. 4 August 2011

Monetary penalty notices are reserved for the most serious and negligent data protection breaches. The majority of monetary penalty notices to date have been served on local government data controllers. These have included:

- Monetary penalty of £120,000 issued to Surrey County Council after sensitive personal data was emailed to the wrong recipients on three separate occasions. June 2011
- Monetary penalty of £80,000 issued to Ealing Council following the loss of an unencrypted laptop which contained personal information. February 2011
- Monetary penalty of £70,000 issued to Hounslow Council following the loss of an unencrypted laptop which contained personal data. Hounslow Council did not have a written contract in place with Ealing Council or monitor their procedures for operating the service securely. February 2011

- Monetary penalty of £100,000 issued to Hertfordshire County Council for two serious incidents where council employees faxed highly sensitive personal data to the wrong recipients. The first case, involved child sexual abuse and the second involved details of care proceedings. November 2010

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

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.

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.

Consensual audits

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

Year	Number of audits – NHS	Grading	Number of audits – Local government	Grading
2005/6	2		1	
2006/7	4		1	
2007/8	2		1	
2008/9	1		0	
2009/10	2	Amber (2)	3	Amber (2) Not rated (1)
2010/11	6	Amber (1) Yellow (5)	8	Red (1) Amber (4) Yellow (3)
2011/12 to date	1	Yellow	1	Yellow

Figure 5: Number of consensual audits conducted by the Information Commissioner by year with grading – NHS and local government⁴

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

The NHS

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 both the NHS and local government. In a number of NHS

⁴ Gradings were not provided for audits prior to 2009/10

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
	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.
	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.
	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.
	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

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.

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.

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 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

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.

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.

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.

Local Government:

Recurring issues identified in the local government sector through audits have included a lack of records regarding data sharing, a failure to encrypt laptops and mobile media, poor weeding or destruction of records, inadequate systems in place for the monitoring of subject access requests (databases often exist for the recording of requests but frequently these are run in isolation among the different departments of the organisation). In a number of audits the Information Commissioner has been supplied with policies and procedures prior to a site visit but once on site it has become evident that adherence to these policies is not being monitored.

Case study 1 – This audit of a local council identified a number of significant concerns including; a lack of clearly defined responsibilities for data protection compliance, failures to identify and implement controls by which compliance with data protection could be measured and reported, confusion between the DPA and Freedom of Information requests, no common system (capable of providing comprehensive management information) for access to personal data to be tracked across the organisation, the Information Security Policy did not cover the transportation and use of manual files off site, failures to ensure an appropriate awareness by staff of their individual responsibilities for handling data.

Case study 2 – Audit of a local authority identified a number of compliance issues; there was considerable pressure on the single Corporate Governance staff member in post, the organisation was unsure if any DP training was provided to new starters, only 30% of staff questioned were aware of subject access procedures, less than 40% of staff questioned knew to report subject access requests to relevant staff, at the time of the audit several access requests were significantly overdue with no plan in place to resolve them, no monitoring of requests received, no priority to allow staff to respond within 40 days, no formal incident reporting procedure to encompass data protection and information security risks, staff in some areas had no awareness of retention policies, no clear record of who had received training, no highlighting of the new DP procedure for staff, only half of staff questioned felt they had received enough DP training to help them in their role.

Follow up

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.

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.

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

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 letter⁵ 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

⁵
http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_129895.pdf

Commissioner to carry out a data protection audit and encouraging organisations (particularly those newly providing NHS services) to accept.

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.

Less than half (47%) of local government organisations contacted with a view to an audit by the Information Commissioner have agreed. This compares to 71% across the public sector as a whole.

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

Structural changes in the NHS may make defining at this point exactly how far an audit power should be extended difficult as new Commissioning boards, GP consortia and providers emerge. The Information Commissioner is concerned that the ability to serve an assessment notice clearly extends to any provider delivering publically funded NHS services. Members of the public are unlikely to expect a distinction to be made between the options available to audit the practices of their GP's surgery and the options to do the same for a publically funded provider their GP refers them to. The Information Commissioner is therefore of the view that

there is a clear case to extend the power to serve an assessment notice to cover all public, private or third sector organisations who deliver publicly funded health care services in the UK.

The 'Code of Recommended Practice for Local Authorities on Data Transparency'⁶ includes a definition for 'local authority' which provides a logical basis for setting out the scope of the organisations subject to the assessment notice power in local government. This includes a cut off for Parish Councils with an income below £20K.

Resource for conducting audits

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.

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.

⁶ <http://www.communities.gov.uk/documents/localgovernment/pdf/1997468.pdf>

Summary

The evidence set out above clearly demonstrates that the NHS and local government are two areas 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.

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.

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.