Good Practice

Audit outcomes analysis

NHS – February 2010 to July 2012

This report is based on the final audit reports the ICO completed for audit visits carried out in the National Health Service (NHS) during the time period above. No individual organisation is named in the report.

Assurance ratings

When conducting an audit, we assess the arrangements an organisation has in place for complying with the Data Protection Act 1998 (DPA) and the extent to which they are being adhered to.

We then give an overall ‘assurance rating’ (as described below) indicating the extent to which it seems that the key risks to non-compliance are being managed effectively.

Assurance rating	Description
High assurance	Limited scope for improving existing arrangements. Significant action unlikely to be required.
Reasonable assurance	Some scope for improvement in existing arrangements.
Limited assurance	Scope for improvement in existing arrangements
Very limited assurance	Substantial risk of non compliance with DPA. Immediate action required.

Overall audit assurance ratings

During the period, we audited 15 NHS Hospitals and Trusts and gave the following assurance ratings.

Audits completed during the period	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
15	1	10	4	0

- 67% fell within the reasonable assurance range.
- 27% fell within the limited assurance range.
- One high assurance rating was awarded.
- The trend indicates a year on year improvement in the assurance ratings awarded which suggests improvement in the management of key information and data protection risks.

Scope area assurance ratings

ICO audits can cover a number of key scope areas (described below). We give an assurance level of the overall performance in each scope area. During the period, we gave the following assurance ratings.

Scope area	Rating	Total
DP Governance The arrangements and controls in place to ensure compliance with the DPA.	High	2
	Reasonable	8
	Limited	3
	Very limited	0
Records management The processes in place for managing both electronic and manual records containing personal data.	High	1
	Reasonable	5
	Limited	1
	Very limited	0
Requests for personal data The procedures in place to deal with any requests for personal data.	High	0
	Reasonable	3
	Limited	2
	Very limited	0
Security of personal data The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.	High	0
	Reasonable	11
	Limited	4
	Very limited	0
Training and awareness The provision and monitoring of staff DPA training and the awareness of DPA requirements relating to their roles and responsibilities.	High	2
	Reasonable	7
	Limited	3
	Very limited	0
Freedom of information requests* The arrangements and controls in place to ensure compliance with the FOI Act.	High	0
	Reasonable	0
	Limited	0
	Very limited	0

** Only introduced as a scope area in 2011*

Common areas of good practice

We observed good practice in **governance** and **training and awareness**. In particular:

- the existence and periodic review of data protection policies and procedures, which are made available to all staff; and
- the implementation of data protection and information governance training programmes.

Common areas for improvement

A common area for improvement is **security of personal data**. In particular we noted:

- poor network access controls;
- a lack of specialised information security and systems training; and
- the absence of effective information security compliance testing or asset management.

General findings and observations - good practice

The following areas of good practice were observed across the NHS.

- ✓ Information governance frameworks in place and clear management strategies for information governance and data protection.
- ✓ An information governance strategy supported by relevant policies and procedures which were reviewed regularly, published and available to all staff.
- ✓ Data protection training programmes implemented and executed.
- ✓ Information risk registers in place and risk management embedded within the organisation.
- ✓ Incident security management policies in place.

Detailed findings and observations - good practice

- ✓ Transferable training logs for junior doctors that moved round various hospitals within a Trust that gave assurances of data protection and information security competency regardless of working location.
- ✓ Security Incident Management systems and tools developed which tracked and reported on security incidents. Overall accountability assigned for incident management through the information governance framework.
- ✓ Information governance micro sites and communities set up within intranet sites for discussion forums and task groups to share data protection issues and good practice ideas.
- ✓ Automated systems developed to capture and report on staff acceptance of data protection and information security related policies and trigger periodic reviews.
- ✓ Data protection and information governance training programmes extended to accommodate out of hours or on call employees by offering flexible training times and locations. Also, training content adapted with specific practical examples and scenarios at departmental level.
- ✓ Uniform application of the risk management scoring matrix across all risk registers, for example information asset registers, information risk registers and incident reporting systems.

Detailed findings and observations - for consideration

Overall controls could be enhanced with the introduction or development of the following.

- Delivery of specialised, role based training for key personnel in data protection and information governance.
- Extension of security encryption for *all* removable media and mobile devices.
- Active internal data protection policy document controls, compliance monitoring and reporting. Key performance indicator results communicated at Board level.
- Password security procedures for all systems and effective controls to minimise password sharing practices.
- Review of existing manual record storage and transportation policies to improve security of manual data. Consider current transportation methods between departments/sites and secure storage of records whilst on patient wards.
- Strengthening of subject access request processes by assigning ownership and accountability, monitoring compliance with legislation and providing specialised role based training as required.