Good Practice

Audit outcomes analysis

Health – August 2012 to January 2014

On 1 April 2013 the structure of the NHS in England changed. Primary Care Trusts (PCTs) were abolished and replaced with Clinical Commissioning Groups (CCGs). CCGs can commission any service provider that meets NHS standards and costs. Also, as part of a drive to reduce the use of identifiable patient information, the CCGs have been encouraged to use pseudonymised and anonymised data. While a development that we welcome, in the short term it has caused significant problems for the reformed NHS. We have worked with local and national organisations to ensure that data protection obligations have been understood and honoured but in such a way that they have not become a burden for the new health service.

ICO colleagues have worked proactively with the Health and Social Care Information Centre (HSCIC) to deliver an incident reporting tool. We have been encouraged by some of the improvements made for the Information Governance Toolkit (IGTK) version 11, for example, the guidance on auditing evidence used for the requirements and the systemic amendment made which prevents roll over of level 3 maintenance criteria. We believe that together these should help to improve the robustness of self-assessments and therefore the consideration of personal data.

During 2013 ICO staff participated in HSCIC led IGTK workshops along with other NHS and third party information governance professionals. The purpose was to provide our feedback on working with the IGTK as a Regulator and to learn from other information governance colleagues.

In deciding which organisations we approach to offer the opportunity to participate in our audit programme we monitor the trends logged by our enforcement department:

ICO Enforcement Trends

In addition to monitoring trends we also carry out risk assessments to ensure we target our work in the areas of highest risk.

This report is based on the final audit reports we completed for audit visits carried out in the health sector during the time period above. No individual organisation is named in this 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 provide 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	Considerable 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 19 health related organisations, including NHS Trusts, Health Boards, Health & Social Care Trusts and companies with a focus on health services. We gave the following assurance ratings.

Audits completed during the period	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
19	1	9	8	1

- 5.2% fell within the high assurance range
- 47.3% fell within the reasonable assurance range.
- 42.3% fell within the limited assurance range.
- 5.2% fell within the very limited assurance range.

This breakdown shows that as a result of our audit activity we have identified room for improvement at the all but one of the organisations we visited.

Background

Organisations we visited in England are required to submit an annual NHS IGTK return to HSCIC (Connecting for Health prior to April 2013). The IGTK is essentially a self-assessment return and is used to ensure that the organisation is complying with Department of Health NHS Information Governance policies and standards and has the foundations of an Information Security Management System.

In September 2011 the Information Commissioner in conjunction with Sir David Nicholson, NHS Chief executive wrote to all Chief executives and Directors of Finance within the NHS outlining some key information governance requirements and encouraging participation in our audit programme.

To ensure our audits are consistent with IGTK guidance, we have mapped IGTK controls against our own audit process. This ensures that we cover appropriate and relevant content and build upon standards mandated by the Department of Health. Where possible, within this feedback we have documented the relevant IGTK requirement and provided a commentary about our experience.

Individual organisations IGTK submissions are publicly available and can be viewed by accessing following link **https://www.igt.hscic.gov.uk/**

Regional health organisations have their own regional processes to ensure IG compliance, Scotland still make use of the IGTK, although not on a mandatory basis, Wales use the Caldicott Principles Into Practice (CPiP) and Northern Ireland have Control Assurance Standards.

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.

Each scope area contains within it a number of specific controls. Each control is individually scored to provide an overall assurance rating for the scope area being assessed. Where information risks are identified within a scope area we make recommendations to increase assurance ratings against specific controls.

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	1
	Reasonable	5
	Limited	3
	Very limited	1
Records management The processes in place for managing both electronic and manual records containing personal data.	High	0
	Reasonable	7
	Limited	5
	Very limited	0
Requests for personal data The procedures in place to deal with any requests for personal data.	High	0
	Reasonable	2
	Limited	1
	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	9
	Limited	6
	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	1
	Reasonable	1
	Limited	2
	Very limited	0
Data Sharing* The design and operation of controls to ensure the sharing of personal data complies with the principles of the DPA.	High	0
	Reasonable	3
	Limited	2
	Very limited	2

Our audit observations

Data protection governance and management

The IGTK requires that there is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda. The Information Governance (IG) agenda is supported by confidentiality and data protection skills, knowledge and experience which meets the organisation's assessed needs.

We noted that information governance and management were embedded within organisational frameworks. Information Governance can broadly be defined as the aims and strategic direction defining the organisations attitudes towards the handling of personal data, whilst management may encompass the plans required to achieve these aims and the building of appropriate structures to deliver them.[1] Consistent with IGTK guidance cross organisation groups comprising of specialists including data protection, records management, IT, clinical governance and Caldicott roles were used to provide appropriate IG structure.

A board-level Senior Information Risk Owner (SIRO) is required in each organisation and a senior Information Asset Owner (IAO) should be designated for every separate database or other major information asset.[2] We noted that many SIROs adopted a hands-on role, chairing cross organisation IG groups and/or leading on IG initiatives.

Example:

We observed that the majority of organisations had difficulties in keeping track of and maintaining accurate records of IAOs in post. In addition, IAOs were often lacking a full understanding of their responsibilities, and in many cases had not received appropriate training to support the key nature of their role.[3]

IAOs are essentially the eyes and ears of the SIRO; particularly, due to the size and complexity of some Trusts there is a risk that without proper training and engagement by IAO the SIRO will not derive an accurate informed view of information risk required for Board level reports or compliance statements.

There are many resources (including those provided by the IGTK and the Cabinet Office's "Protecting Information" series of online training) devoted to the development of SIRO and IAO roles. IAO development is further supported by various professional qualifications covering the Information Governance agenda and the National Archives who deliver training to support these roles.

All organisations had data protection policies and procedures, which were kept under review and made available to all staff. However, we noted that compliance

[1] ISACA, Cobit 5 principle 5
[2] HSCIC IG Toolkit resources, NHS Information Governance Assurance Framework
[3] Data Handling procedures across Government, Mandatory minimum measures, 5 'Roles'

with such policies was not always effectively monitored, for example through the use of occasional spot checks, staff confirmation of understanding or the use of policy delivery software.

Records Management

The IGTK requires that procedures are in place for monitoring the availability of paper health/care records and tracing missing records and that all information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.

Example:

At one Trust we witnessed the trial of Trust issued laptops being used by community workers. These enabled staff working in the community to access and update patient records in real time and ensured that delays in updating electronic records from paper based records were eradicated.

It also allowed those staff members to have access to Trust systems and emails, enabling them to keep up to date with IG updates, and reduced travelling costs by minimising the number of visits community staff had to make to Trust sites to deposit updated manual patient records for input onto the system by data entry clerks.

The laptops being used by community staff were fully encrypted and asset tagged. Access to Trust systems was via a secure Virtual Private Network (VPN), with device usage authorised only in line with Trust policies. The scheme also had full Trust IT support.

We noted that the project had been included on the Trust's risk register, indicating a well thought out process and an awareness of the risks involved.

We found that all organisations had a system in place to track health records; however some Trusts were using the tracking software more effectively than others. Some organisations were ensuring all files were tracked before they left the library and when they arrived at their destination, while others did not track files until they arrived at their destination. In addition to this not all of the organisations we audited were conducting missing/duplicate file audits, or reporting the findings to the Information Governance Team to allow proper oversight by staff and forums with specific data protection responsibility.

In relation to the security of health records we found disparity in how each organisation protected health records, while in records libraries and during transport to wards and outpatient clinics. Some Trusts controlled access to the libraries via a key code door lock, with difficulty in controlling the passing of the door code between staff. Others restricted access, through the use of swipe cards with access limited by role with regular access right audits being carried out to ensure the minimum number of staff had access to the records library. There

were also great differences in the records libraries, with some being over capacity and others being well managed through a system of weeding and scanning. It was noted that where relevant to the audit scope there was very little in the way of fire or flood protection in place for paper records.

We observed files being moved around Trusts in trollies; some Trusts requested that a member of staff collected the trolley while others delivered the trollies direct to the clinic. The common area of concern was that the majority of these trollies were not locked.

Example:

We have seen Radio Frequency ID tag systems (RFID) installed at a number of Trusts for asset tracking purposes, which are also being utilised to provide the ability to track medical records and therefore prevent their loss.

The system employs RFID tags attached to patient records, and a network of sensors which track them as they pass within read-range and automatically record the last zone entered. This allows file movements to be tracked and recorded in a central database, which enables less structured filing and a more compact library.

Searches for records inside the library and those in circulation are made easier with mobile guns which scan and detect records' precise location. These can be programmed with clinic pull-lists, or missing records logs for more effective searches outside the library.

The use of the tracking systems such as this should allow Trusts to reduce the volume of missing records, and consequently the number of temporary files and the risk of duplicates.

Security of Personal Data

The IGTK requires that:

- a formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed.
- there are documented information security incident/event reporting and management procedures that are accessible to all staff,
- operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
- Information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
- there is a requirement that business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service-specific measures are in place

We noted that all of the organisations audited during the period had appropriate

information governance related risk registers, risk assessments which were regularly reviewed at board level, demonstrating that the organisations were identifying and addressing potential weaknesses in the processing of personal data. Common areas for improvement were, out of date or incomplete Information Asset Registers and poorly trained Information Asset Owners.

All organisations had security incident management systems and tools in place which tracked and reported on security incidents (including personal data incidents). Overall accountability had been assigned for incident management through the information governance framework.

On the 31 May 2013 a joint HSCIC and ICO personal data breach reporting initiative went live. This allows NHS users to use one tool, hosted by the IGTK to report incidents to both the ICO and the NHS' own regulatory bodies and it is hoped this will reduce duplication of effort.[4]

Example:

We observed the use of Fax machines at the majority of organisations we audited. However there were vast differences in the security of these machines and the procedures for using them.

Most organisations had a faxing policy and procedure, and a small number of these had located fax machines in secure rooms to ensure that a limited number of staff had access to such machines.

The ICO has concerns about the use of Fax machines due to the fact that human error cannot be totally eradicated.

Our guidance on the secure use of fax machines advises that organisations sending personal information by fax should:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.

- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

[4] The ICO Enforcement Intelligence Team is working closely with HSCIC to ensure that the reporting mechanism within the IG toolkit mirrors the ICO's own approach to risk categorisation.

- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.

- Ring up or email to make sure the whole document has been received safely.

- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

A number of organisations visited did not have effective asset management in place for IT hardware and software; this raises the risk of the business not knowing what devices are in circulation and therefore not becoming aware if one is lost or stolen.

We noted that there was a lack of regular password changes, reportedly and in part, due to legacy systems not having the functionality to routinely enforce password policies. Whilst we understand the necessity for straightforward access to essential systems in a clinical environment, simple password controls are a widely accepted and essential user access control; without which, prevention of inappropriate access, identification of user activity and construction of audit trails will be problematic.[5]

All of the organisations audited during the period had a starter/mover/leaver process in place; however there was not routine monitoring across all of the organisations in relation to access rights to ensure that access to personal data was appropriate to role.

We also found a lack of end point control in some organisations where active USB ports and disc drives had not been locked to prevent the downloading/uploading of information. End point control should be applied to restrict all but essential ports and drives where a business case is signed off at an appropriate level and the access is kept under review. Inappropriate attempted use of USB ports should also be logged and reviewed to assist with the delivery of training and awareness.

There were business continuity plans in place for electronic systems however there were generally no continuity plans in relation to paper health records.

We did note however that there was an absence of effective information security compliance testing. For example, a pragmatic programme of monitoring staff adherence to policies and procedures can further develop management understanding and will contribute to developing more effective controls.

[5] HSCIC IG Toolkit, Guidance 11-305 'Access controls and functionality'

Training and awareness

The IGTK requires that mandatory training procedures are in place and all staff are appropriately trained. We observed the use of the HSCIC (Connecting for Health prior to April 2013) e-learning modules; the common difficulty facing Trusts was monitoring and enforcing training uptake and completion. We were pleased to note a high level of staff awareness of the need to keep patient data secure. However, ICO Enforcement case work trends underline the need to regularly revisit this area with staff.

Senior Management should consider what measures are in place to ensure that mandatory training is completed by all staff. We observed that in some organisations, the SIRO and Caldicott Guardian were instrumental in monitoring take up and completion of IG training. Subsequent email reminders were issued to staff where appropriate.

In addition to this, some Trusts have demonstrated good practice by developing stand-alone bespoke training packages to complement the standard e-learning package, while other Trusts rely solely on the HSCIC materials.

We noted that, in a minority of organisations, IT security training was not always undertaken at induction or annually. Poorly trained staff will increase the risk of breaches occurring as do inappropriate access rights.[6]

Example:

The majority of organisations we visited utilised the on-line training available on the IG Toolkit website. However there were vast differences at some trusts, with a few offering bespoke training packages in addition to the on-line training, while others provided leaflets to staff in an attempt to raise awareness without providing any formal training.

At all organisations there was confusion over how best to ensure that junior doctors and medical students completed relevant data protection training.

This is an issue which was highlighted in an ICO News Release. Sally-Anne Poole, ICO Enforcement Group Manager said:

"If organisations are employing temporary or agency workers into positions that involve the handling [and sending out] of personal information then they must make sure these staff have received adequate data protection training."

During the planning stages of three of our audits we surveyed 152 members of staff, by using an online survey, to enable us to reach a greater number of frontline staff to establish their understanding of basic data protection concerns, organisation policies and procedures. The results demonstrated the following:

[6] See ICO Enforcement Trends link

- 88% of the staff surveyed had read and understood the Data Protection Policy in place within their organisation.
- 94% of the staff surveyed had completed Data Protection training within the 12 months before the audit was conducted.
- 95% of staff felt they had sufficient awareness of the Data Protection Act to enable them to carry out their role.

We hope to make greater use of on-line surveys in the future to enable us to reach as many staff members as possible.

Data Sharing

The IGTK requires that:

- all transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed;
- that technical and organisational measures adequately secure these transfers;
- where appropriate, protocols governing the routine sharing of personal information have been agreed with other organisations;
- all new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner; and
- there is compliance with IG security accreditation, information quality and confidentiality and data protection requirements.

We introduced the data sharing scope item in August 2012 to align with our Data Sharing Code of Practice which can be found at the following link:

Data Sharing Code of Practice

We noted that the majority of organisations have data sharing agreements in place to allow for lawful sharing of patient information and they were making people aware of any sharing using fair processing notices. However, we found that many organisations did not log the agreements in place and were not routinely monitoring the information being shared.

Example:

At one Trust we visited, the tendering and procurement process included the creation of an evaluation panel to assess the Data Protection practices and/or security arrangements in place before a contract was awarded. In addition, a data sharing agreement was produced to supplement the contract to ensure data protection considerations were addressed comprehensively.

It is also important that agreements are periodically reviewed to establish whether the agreement is still needed and the extent to which personal data still needs to be shared.

Example:

One of the organisations we audited had a regional data sharing agreement in place. The agreement covered personal data shared between all health and social care providers in the region and included disclosures to the police. All parties named on the data sharing agreement sent one member of staff with IG responsibilities to a regional quarterly IG meeting to ensure that all parties were aware of information flows around the region and ensuring that the data sharing agreement was fit for purpose.

In addition, organisations were not regularly reviewing information flows via a mapping exercise linked to the Information Asset Register and were not always carrying out appropriate Privacy Impact Assessments.

http://www.ico.org.uk/news/blog/2013/nhs-changes-ico-data-protection

Follow Up Audits

We carry out follow up audits in line with standard audit practice for any audit that did not achieve high assurance. Follow up audits usually take place between six to nine months after the initial audit. During the period we carried out follow up reviews with 11 NHS Trusts and 2 non NHS health service providers.

We listen to the feedback that organisations give us, whether this is during or after the audit process and we make pragmatic recommendations which we discuss and agree with the organisations concerned. As a result of feedback we received we changed the follow up process in order to make the process less labour intensive for organisations. We no longer re-assess the audit assurance ratings, instead we ask for assurance from a senior board member that steps have been taken to meet the audit action plan that we provided after the initial audit.

The follow up reviews have demonstrated that organisations take on-board the learning in our reports and take remedial actions to mitigate risks that we have identified.

Audit Feedback

At the end of the audit process we request feedback from those we have audited. Some of the feedback we have received is detailed below:

"What impact has the ICO audit had on data protection compliance?"

- A renewed focus on audit beyond the requirements and aspirations of the IG Toolkit.

- The audit has highlighted various areas where data protection

practices could be improved, the ICO has provided us with a useful action plan which we will work towards completing.

- The ICO audit reinforced much of the work that the information governance team at the Trust had been carrying out over the last few years. The recommendations gave weight to some of the areas that the IG team had been keen to pursue and this helped to progress these quicker.

- The ICO audit has given us great feedback on our processes already in place to comply with Data Protection, and it has certainly raised awareness to our senior members of staff in that they now realise the benefits and importance of good data protection and compliance within our organisation.

"Do you have any other comments to assist us in improving the quality of our audits?"

- The ICO audit is quite a daunting process and staff were quite stressed at the short amount of time they had to collate all their evidence together. The audit had occurred just over a bank holiday and a number of staff had been on leave. However audit staff were flexible and worked well with all staff concerned. The preliminary meeting and accessibility of ICO staff was welcomed to confirm and check the nature of information that we had to provide and on-going queries.

- Not really - the scope and process were clearly defined well in advance, which enabled us to manage the interview process efficiently, given the number of staff involved. As far as I know all participants were happy with the audit process, and I have received no adverse comments. Subsequent informal discussions with the Lead Auditor have been extremely useful - not within the scope of the audit, but it is useful to have a contact for advice who has specific knowledge of the organisation.

Further information

All of our health sector outcome reports can be found at the following link:

http://www.ico.org.uk/for_organisations/sector_guides/health