Hambleton, Richmondshire and Whitby
Clinical Commissioning Group

Role and Responsibilities of the Information Asset Owner

Authorship:	Chris Wallace
Review Date:	*August 2014*
Target Audience:	Information Asset Owners
Version Number:	*1*

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

CONTENTS

1 Introduction

The Information Asset Owner (IAO) is a mandated role, and the individual appointed is responsible for ensuring that information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

An Information Asset Owner reports to the Senior Information Risk Owner (SIRO), who in turn reports to the Accounting Officer or the Chief Executive. Information handling is reported on in your organisation's statement of internal control, and the IAO is expected to provide information to go into that report.

The role was created following the Government's Review of Data Handling in Government (DHR) in June 2008, which also established mandatory minimum measures for personal data handling in Government. You can find full details in HMG IA Standard No 6: Protecting Personal Data and Managing Information Risk. This incorporates the Data Handling Review and included and replaces the minimum mandatory measures.

Although it was created out of the DHR, which initially focused on personal data handling, the role is equally important for any sensitive information processed by your organisation, whether or not it includes personal information. The IAO also needs to manage information assets to comply with statutory obligations (such as Freedom of Information Act, the Public Records Act and the Data Protection Act.

Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information you hold, how important it is, how sensitive it is, how accurate it is, how reliant you are on it, and who's responsible for it. It helps ensure that you can use the information you need to operate transparently and accountably, for example to meet open data standards, to unlock previously unavailable data and to improve public service.

1.1 What is the purpose of this guidance?

The three Acts identified above give an overview of why the IAO role was created and what you are expected to achieve. But Information Asset Owners have asked for more information about what that might mean in practice. This document provides a good starting point for IAOs, giving practical guidance on:

- identifying information assets
- managing information risks
- your responsibilities
- how to achieve them
- who can help you
- how to know if you are doing your role well.

It fits into a wider package of support for your role, for example baseline training for IAOs, knowledge-sharing events, and continuing work to help define what we mean by an information asset.

1.2 Who is this guidance for?

This guidance is primarily aimed at Information Asset Owners. It may also be useful for Information Asset Administrators and for information management (IM), information assurance (IA) and IT teams – for example Heads of Knowledge and Information Management, Departmental Record Owners, Heads of IT and IA – to help them to understand the support they may be called upon to provide.

It could also be useful for project managers when initiating projects, particularly those likely to be subject to Privacy Impact Assessments (PIAs).

2 Just appointed?

2.1 First steps

- Have you done Information Risk Management Introductory and Foundation courses available online through the Information Governance Training Tool.
- Have you read Managing Information Risk?
- Have you contacted the IMT IG, Security and Governance Team to enquire about resources that are available to you for the completion of your role?

2.2 Key principles

Your role is about managing **information** not systems.

The initial driver for establishing the role of the IAO was to ensure that Personal Data was identified and securely handled. However, you also need to ensure you are managing the handling of other categories of sensitive or important information that the organisation relies on too. This involves making sure that it can be used in the way that you need, for as long as you need.

You are responsible for ensuring that information is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards apply. But you are equally responsible for ensuring that its value to the organisation is fully realised, and that it is used appropriately, and within the law, for public good. You will also need to ensure that information is managed appropriately following change (see Appendix B).

Your role is about providing assurance and making sure that action is taken. But that doesn't mean you have to do everything yourself – in fact, much of the role is about understanding and where necessary coordinating the activities of others within the

organisation who have specialist areas of responsibility. Your departmental IAA's, IT, Security and Records Management functions are key contacts in supporting you in the role. However, if you delegate responsibility for ensuring actions are taken, you must make sure that this is properly co-ordinated and that there are clear reporting chains that everyone understands. You can delegate responsibility to particular areas that can support you in your role but you and your SIRO retain the accountability for proper information management and handling.

You may need to work with other IAOs in your organisation to ensure your information is properly protected and their value to the organisation fully realised.

2.3 What is an information asset and what assets are you responsible for?

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Your SIRO will decide what information assets you are responsible for. This should not just be a list of systems to manage, but should focus on the information that needs to be managed within those systems. This could cover both sensitive personal data and non-personal information that is critical to business. It could be held in paper as well as electronic formats.

When you are appointed you need to discuss and agree performance metrics. Some of these will be directly related to the need to demonstrate compliance with mandatory requirements to central government, but others may be specific to your organisation. Where practical, you should discuss with your SIRO or Information Governance Team what you will be expected to report back on.

3 Information risks to Manage

As an Information Asset Owner you will need to assure against:

- Inappropriate access to, or disclosure of, protectively marked or personal data by staff, contractors and outsiders, whether accidental or deliberate;
- Internal threat – staff acting in error or deliberately, or external parties getting your information illegally and exposing it/acting maliciously to defraud you or your customers;
- Information loss – particularly during transfer or movement of information, or as a result of business change;

- Loss of ready access to information;
- Loss of digital continuity – i.e. losing the ability to use your information in the way required when required. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information – and how long you need to use and keep it – is often different to the lifecycle of the IT system that we have to access and use it;
- Poor quality of information and poor quality assurance, for example, of datasets;
- Poor change management – business needs change, systems change, your information risk appetite may change, so you need to keep your policies and processes in step accordingly; and
- Not maximising the public benefit from information (leading to a waste of public money and poor service delivery).

4 Your responsibilities

Your role is to ensure that the information in your charge is properly protected and its value to the organisation fully realised. This section of the guidance provides examples to get you thinking about your responsibilities and how that might look in practice. Specific responsibilities for an IAO are detailed within Appendix A. Some of your responsibilities require you to take action, others simply to assure that action is being taken by others (such as your IMT and IG teams).

You have five responsibilities:

1. Lead and foster a culture that values, protects and uses information for public good.
2. Know what information the asset holds, and what information is transferred in or out of it.
3. Know who has access and why, and ensure that their use of the asset is monitored.
4. Understand and address risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are appropriately managed
5. Ensure the asset is fully used for the public good, including responding to access requests.

You need to be able to answer the following questions:

- Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented within the Information Asset Register (IAR) and shared with your SIRO and others who need that information?

- Have I assessed and logged information risks to those assets?
- Do I have a plan for managing risks, and maximising opportunities for using my information assets for the public good?
- Do my team(s) and third parties understand their roles and responsibilities in managing those risks and opportunities?

Your IMT and IG teams are a great resource and can support you to provide much of that assurance. You need to tell them your business requirements so that they can include them into their operational IT, protective security and information management.

4.1 Lead and foster a culture that values, protects and uses information for the public good

What you need to do	**How you might do this**
• Attend (and pass) training – when you're appointed and annually (at a minimum) • Actively contribute to your department's plans to achieve and monitor the right information handling culture • Ensure the handling of your information assets complies with the Data Protection Act and your department's compliance mechanisms and policies • Understand and document the business value of the information assets you are responsible for.	• Meet with other IAOs in your organisation to share ideas and talk to your Knowledge and Information Management team • Make sure that people who use your information assets understand the rules and are aware of the consequences of non compliance. Explore using line management responsibilities – appraisals and objectives setting – to monitor this • Talk to your SIRO or IG Team about what you can do to contribute to departmental plans for culture change • Set up a 'lessons learned' log, so if things go wrong you can learn from them and ensure that policies and practices are changed • Talk to IMT and IG Team to ensure appropriate physical, procedural and personnel security

4.2 Know what information the asset holds, and what information is transferred in or out of it

What you need to do	How you might do this
• Understand and address risks to your information assets, and provide assurance to your SIRO • Know who has access to your information assets and why, and monitor use • Understand whether a delivery partner or supplier has a dependency on your information to deliver a service • Approve and minimise transfers • Monitor the allocation of users' rights to transfer personal information to removable media • Approve arrangements so that information put onto removable media is minimised and protected • Make sure your information assets are fully used for the public good, including responding to access requests.	• Document your understanding of your information assets (within the Information Asset Register) ○ What the assets are – what they cover, their content, what's sensitive and/or protectively marked and what personal data you're responsible for). Work with your IG team to document; ○ The value of your information assets to the business – now and in the future. How important are they, and why? What would be the impact of losing or mishandling them? As part of this process you should consider the benefits of increasing access, or of information re-use; ○ Your usability requirements for those assets – who needs to be able to find them, how do you need to work with them, to maintain the understanding and trust of that information? What retention and disposal schedules do you need? • Keep a record of all staff and contractors with access to records containing personal data – or who handle records containing personal data. Ensure a process is in place to remove that access as soon as it is no longer required • Manage agreements on the sharing of personal information between organisations • Keep written records of the decisions you agree with your IMT, IG and security teams

4.3 Know who has access and why, and ensure their use of the asset is monitored

What you need to do	How you might do this
• Ensure that you keep a record of individuals with access to, or who handle, records containing personal data • Keep a log of access requests	• Make sure you understand your organisation's policy on the use of the information assets you are responsible for • Make sure that processes are in place for approving access to information systems and that these access lists are reviewed regularly • Talk to your IG Team to ensure appropriate policies to protect physical, personnel and information security are in place

4.4 Understand and address risks to the asset, and provide assurance to the SIRO

What you need to do	How you might do this
• Ensure that significant correspondence about information risk handling are placed on the corporate record • Contribute to the department's risk assessment. To do this, the IAOs should identify and, where appropriate, formally accept significant risks introduced when personal information is moved from one organisational unit, system element, medium or location to another • Make the case where necessary for new investment to protect the asset • Ensure all risk decisions taken are demonstrably in accordance with risk management policies established by the SIRO • Make risk decisions where users believe it is not possible to comply with policies or controls, consulting	• Make sure you are aware of the full range of risks – see section 3 above • You defined your usability requirements in section 4.2 above. Use this information to assess risks and opportunities: ○ Understand how to maintain your digital continuity – identifying the management processes and technologies you need to satisfy your usability requirements ○ Identify the technology that your information is dependent on to remain usable. ○ Identify the risks to the information asset that could arise from changes, for example technology change (changing suppliers, systems and so on) and organisational change (e.g. sharing agreements, who has access to the information)

others as necessary, and ensuring the decision and the reasons behind it, are placed on the corporate record	• Read your organisation's Risk Policy – a mandatory document for all government departments and agencies. This should indicate where losses of confidentiality, integrity and availability are likely to have the most critical impacts on your business, and where the greatest proportion of your mitigation should be focused • Talk to your IG Team about how the risk policy applies to the information assets you are responsible for

5 Further reading

Familiarise yourself with the policies, standards and procedures in place within the organisations:-

- Risk Management Policy
- Information Governance Framework
- Information Governance Policy

For more information about how you can assure against the risk of losing the use of your information assets over time and during periods of change, visit nationalarchives.gov.uk/digitalcontinuity

For more on why it matters, read What Does Digital Continuity Mean for You? An Overview of the Benefits

nationalarchives.gov.uk/documents/information-management/an-overview-of-the-benefits.pdf

Managing Information Risk gives a good overview of broader information risks, case studies, checklists and potential sources of assurance
nationalarchives.gov.uk/documents/information-management/information-risk.pdf

Appendix A: Information Asset Owners Responsibility Table

Aspects	Responsibilities	Guidance
Lead on and embed a culture that values, protects and uses information for the success of the organisation and benefit of its customers	To understand the organisation's plans to achieve and monitor the right NHS Information Governance culture, across the organisation and with its business partners.	Statutory and Mandatory training is provided via the CBLS system for all training apart from Information Governance. Information Governance Training is provided through the Information Governance Training Tool. Ensure all IG requirements are part of any tendering process and contracts awarded details, and are appropriately reflected in contracts to which the organisation becomes party. Ensure that CSU Project Board approval is sought for any new information systems either paper or electronic.
	To take visible steps to support and participate in that plan (including completing own training)	IAOs must undertake training in accordance with Information Governance Training Tool, this requires the completion of the appropriate NHS Information Risk Management Modules. To include IG requirements in all business procedures and processes, policies and procedures and make these available as required.
	To ensure that staff understand the importance of effective information governance and receive appropriate education and training	To ensure that completion of IG training is achieved as part of the appraisal process. In addition to determine whether the job role being appraised should be subject to completion of any additional Information Governance Training Modules available via the Information Governance Training Tool. Ensure that third party contracts include the requirement for

		Information Governance training and awareness for 3rd party staff.
	To consider whether better use of any information held is possible, within applicable information governance rules, or where information is no longer required.	Each information asset must be recorded and associated information flows mapped and assessed. At each stage of the information flow consideration must be given to: Is this a justified information flow? Is the purpose of processing this information legal? Is there a legal justification for doing so? Has explicit consent of the data subject been obtained and recorded? Is the information collected fairly? Is the information held securely? Are all transfers/transmissions undertaken securely? Are recipients aware of their information governance responsibilities? These must be notified to the Information Governance Team for assessment to ensure that they are being undertaken on a legal basis. All new information flows must be fully documented and notified to the Information Governance Team before they are implemented.
Knows what information the asset holds, and	To maintain an understanding of 'owned' assets and how they are used	IAOs must ensure that all departmental information assets are recorded on the corporate information asset register and that associated information flows are mapped. These must be kept up to

what information enters and leaves it the asset and why		date and re-assessed on a regular basis. Departmental Business Continuity plans must be put in place in case of an incident or event that makes those information assets unavailable for used for a period of time. These must be proportionate to the impact of the non-availability on the business. Need to include in the corporate business continuity plan and ensure that information governance processes are included in all processes where business continuity plans are invoked. All Business Continuity Plans must be recorded on the departmental information asset register.
	To approve and minimise information transfers while achieving business purposes.	Document all current information flows and assess as detailed above.
	To approve arrangements where it is necessary for information to be put onto portable or removable media like laptops, tablets and USB sticks and ensure information is effectively protected to NHS information governance standards through appropriate encryption.	To ensure that Data Protection, Confidentiality and Caldicott requirements are met and adherence to minimum security measures and encryption (including electronic transfer) policy requirements is achieved. Whilst providing technical controls is the responsibility of the Informatics Dept, ensuring staff compliance is the responsibility of the IAO's.
	To approve the information disposal mechanisms for the asset	Follow the Records Management policy and Records Retention Schedule. Ensure that all disposals of person identifiable information or other confidential information are undertaken in a secure and approved manner.
Knows who has	To understand the organisation's policies on the use	Ensure departmental awareness of Information Governance policies

access to information assets and why, and ensures their use is monitored and compliant with policy.	of information and the management of information risk.	and that staff are aware of how to access them. Information Risks identified at any point should be recorded on the relevant risk register as part of the existing risk management process.
	To ensure decisions on access to information assets are taken in accordance with NHS information governance good practice and the policies of the organisation	Ensuring that access to records in whatever format is approved and that a register is maintained of access given to and removed from electronic and manual systems. An approval process must be established, documented and maintained.
	To ensure that access provided to an asset is the minimum necessary to satisfy business objectives	Access must be provided strictly on a need to know basis only and in line with pseudonymisation requirements.
	To ensure that the use of the asset is checked regularly and that use remains in line with policy	Regular audit of use of information assets is undertaken to ensure compliance. This could be incorporated into the programme of reviewing information flows.
Understands and addresses risks to the asset, and provides assurance to the SIRO	To seek advice from information governance subject matter experts when reviewing information risk	Ensure appropriate guidance is sought from the Caldicott Guardian/Lead, Information Governance Team and Informatics Dept as required.
	To conduct Risk/Privacy Impact Assessments for all new projects that meet the criteria specified by the Information Commissioner	The conducting of a Risk/Privacy Impact Assessment must be considered for all projects. An initial assessment of privacy risk should be carried out at the early stages of a project and where any change of use of existing systems occurs to determine if an assessment is required or to decide which level of assessment is required. Remember it is much easier to implement the appropriate Information Governance and security requirements if identified early

		on in a project. Where they are omitted it could result in a project being halted.
	To undertake quarterly risk assessment reviews for all 'owned' information assets in accordance with NHS Information Governance guidance and report to the SIRO, ensuring that information risks are identified, documented and addressed.	Risk assessment to be undertaken in accordance with corporate risk assessment processes, risks must be reported as part of risk management process and included in regular reports to the appropriate management group.
	To escalate risks to the SIRO where appropriate and to make the case where necessary for new investment to secure 'owned' assets	Risks must be recorded as part of the risk management process and reported to the SIRO. All SUIs, incidents and near misses must be reported and managed via the corporate incident recording system.
	To provide a regular written assessment to the SIRO for all assets 'owned' by them	This report must include as a minimum the following details Training, stakeholders, 3rd parties, business partners, new contracts, significant changes to existing business practices, information sharing including protocols where appropriate.

Appendix B: Data Protection Principles

Guidance on the Data Protection Act should be obtained from the Information Commissioner's Office (www.ico.gov.uk) and from IG Team staff members. The eight principles identified in the Data Protection Act 1998 are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a. At least one of the conditions in Schedule 2 is met; and

b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one of more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country of territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix C: Principles on the transfer of information or responsibilities

Making arrangements for the transfer of information, records and knowledge is a key part of any machinery of government change. However, all too often this aspect is not properly planned for, inadequately resourced and left until it is too late to do everything that needs to be done. Listed below are the eight basic principles that should be followed for a successful transfer.

Further detail on all these areas can be found in The National Archives' Machinery of Government Changes: Guidance on the Transfer of Records, Information and Knowledge.

nationalarchives.gov.uk/documents/information-management/machinery_of_government.pdf

Reinforce Senior Management support

Ensure that senior management understand what needs to be done (including setting an appropriate budget) and the risks to the business if the transfer is not carried out successfully. Failure to transfer information and knowledge effectively between departments can make it impossible to maintain business continuity and can result in the loss of vital information, loss of functionality of digital information, inability to be transparent and accountable and meet legal obligations, inefficiency and substantial additional costs.

Plan in advance

Start planning for the transfer of information as soon as notification that the organisation/function is to be abolished or transferred has been received. Identify desired outcomes – especially the usability of information (or digital continuity requirements after transfer) and test progress against these.

Clarify who is responsible

Establish as early as possible who is going to do the work and form a joint Information Transition Team. Ensure that transferring and receiving bodies and any contractors employed in information related activities (for example, an IT service partner) have a clear understanding of their separate and joint roles and responsibilities.

Decide what to transfer

Decide what information needs to be transferred and to where, for example, information of continuing business or legal value will need to be identified and transferred to the department that is inheriting responsibility for the function/s. Information of archival value may be transferred to The National Archives. Consider information/records in all forms, for example, paper files, information within an electronic records management or email system, websites, intranets, shared drives, databases AND accompanying information such as finding aids, Information Asset Registers or retention/disposal information.

Make provision for the continuity of digital information

Define the usability requirements for information to be transferred, and test against them throughout the transfer process. The receiving organisation needs to ensure the information can be found, opened, used, understood and trusted as required and will need to ensure it receives both files and necessary contextual metadata and has the technology to enable the usability requirements to be met.

Ensure continued compliance with legislation and information security

Clarify responsibilities for Freedom of Information and Environmental Information requests and related complaints and appeals and ensure that handover or guidance notes are prepared. Comply with rules on information security when transferring information and records and conform to the Security Policy Framework for protectively marked material.

Capture knowledge and communicate to staff and stakeholders

Capture the knowledge of staff from the transferring organisation, particularly if they are not transferring with the function and make as much information as possible about the changes available to staff in both organisations. Plan communication with customers and end-users.

Take advantage of opportunities for savings and increased efficiency

Capitalise on opportunities to increase efficiency and make savings, for example, shared service options could be considered for storage/electronic systems, information that is not required could be deleted rather than transferred.

Appendix D: Equality impact assessment tool

To be completed and attached to any policy or guidance document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• **Race**	No	
	• **Disability**	No	
	• **Gender**	No	
	• **Religion or Belief**	No	
	• **Sexual Orientation**	No	
	• **Age**	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**		
6.	**What alternatives are there to achieving the policy/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

If you have identified a potential discriminatory impact of this policy or guidance document, please refer it to the Information Governance Manager, together with any suggestions as to the action required to avoid/reduce this impact.

Retain the completed form with the master copy of the document to demonstrate that the checks have been completed.