Arden&GEM
Health and social care systems support

NHS
Coventry and Warwickshire
Integrated Care Board

# IAO & IAA Handbook

## Key guidance and resources for Information Asset Owners & Information Asset Administrators

Version: 0.1
December 2023

# Table of Contents


| | Page |
|---|---|
| **Introduction** | **3** |
| **Purpose of the booklet** | **3** |
| **Definitions** | **4** |
| **Roles and Responsibilities of an IAO** | **6** |
| **Training for IAOs** | **7** |
| **Information Asset Register** | **7** |
| **Data Flow Mapping** | **8** |
| **Risk Assessment** | **9** |
| **System Level Security Statement and User Access Controls** | **9** |
| **Business/Service Continuity Plan** | **10** |
| **Disaster Recovery Plan** | **10** |
| **System Audit** | **10** |
| **Data Quality** | **11** |
| **Checklist for IAOs** | **12** |
| **Appendix A (SLSP Template)** | **13** |

## 1. Introduction

The role of Information Asset Owner (IAO) was created following the UK Government's 2008 review of data handling within Government against the backdrop of high-profile data losses. The review focussed initially on personal data handling but also covered any sensitive information processed by an organisation.

The recommendations of the review stressed the need to manage Information Assets in compliance with various statutory obligations such as the Freedom of Information Act 2000, Public Records Acts 1958 and 1967, General Data Protection Regulation (GDPR) 2016/679 and Data Protection Act 2018. It suggested that three new roles be established to facilitate the management of information: Senior Information Risk Owner (SIRO), Information Asset Owner (IAO) and Information Asset Administrator (IAA).

The IAO role now forms an integral part of the Data Security and Protection Toolkit which is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

It should also be noted there is a responsibility on project managers/other staff, where these are different to IAOs, to ensure that privacy and confidentiality controls are built into systems at the start of new projects, whether these be new systems or services.

The GDPR now includes a new legal obligation for organisations to conduct a Data Protection Impact Assessment (DPIA) for types of processing likely to result in a high risk to individuals' interests. This is part of the new focus on accountability and being able to demonstrate that the organisation complies with the GDPR.

## 2. Purpose of this booklet

This guidance is primarily designed to aid IAOs around their responsibilities. It will also be of interest to Information Asset Administrators (IAAs).

IAOs perform a crucial role within the organisation. They are an integral part of the Information Governance Framework of the organisation and their role helps to ensure that the organisation complies with national information governance mandatory requirements and guidelines. This document aims to clarify what is required of the role and provide the key resources required for the IAO to effectively manage information risks.

This document provides a good starting point for IAOs, giving practical guidance on:

- identifying information assets
- managing information risks
- your responsibilities

## 3. Definitions

**Information Asset (IA)**
An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and used effectively. Any collection of data required to conduct an organisation's business and the technical equipment to manage this data are referred to as Information Assets. An information asset may comprise of a combination of hardware, software, data, paper records, contracts and skilled resources that together support a business activity. The term Information Asset is very wide ranging in what it can include.

The information assets referred to in this document consist of items such as databases, web servers, software applications, physical paper records, any collection of records such as word documents and spreadsheets.

**Critical Information Assets**
Critical information assets may be defined as those whose continued operation **is essential** to carrying out the core functions of the organisation. Their failure for even short periods of time, may lead to serious patient harm; significant financial or reputational risk to the organisation; as well as legal or regulatory breaches which could affect the organisation's operational ability.

**Key Information Assets**
Key Information Assets are systems or collections of records that are core to the functioning of the business. Their loss or unavailability would have a significant adverse effect on the operations and day to day activities of the organisation.

Other Information Assets which are necessary for the key ones to function may themselves be considered Key Information Assets.

**Senior Information Risk Owner (SIRO)**
This is a member of senior management who has overall responsibility for managing organisational information risk and ensuring appropriate assurance mechanisms exist. Any information related risks identified by IAOs should be entered onto the relevant departmental risk register to enable significant information risks to be reviewed by the SIRO. The SIRO leads and fosters a culture that values, protects and uses information for the success of the organisation and the benefit of its patients.

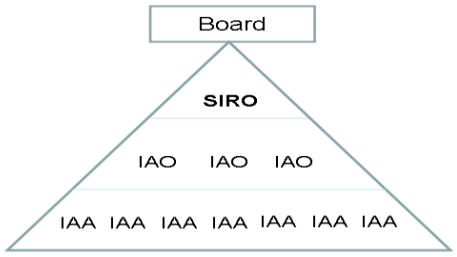
**Information Asset Owner (IAO)**
An IAO is an individual within an organisation that has been given formal responsibility for the security of an asset (or assets) in their work area.

They are responsible for the maintenance of the confidentiality of that asset, ensuring that access to the asset is controlled and that the information is securely kept. They provide assurance that any risks to the information asset are managed effectively. IAOs are directly accountable to the SIRO.

**Information Asset Administrator (IAA)**
Providing support to the IAO, the IAA is the individual or one of a number who uses the information asset on a day-to-day basis. They will generally be more familiar than the IAO with the information, any systems and any risks in their area. This may include responsibilities for:

a) Ensuring IG policies and procedures are followed.
b) Ensuring the principles of and responsibilities for Data Quality.
c) Recognising actual or potential data security incidents.
d) Ensuring that Information Asset Register and Data Flow Maps are accurate and kept up to date.
e) Resolving system issues, including managing and auditing user accounts by setting users up with logons to the system with appropriate access rights according to their role. Audits of user accounts should be undertaken on a defined periodic basis.

The simple diagram below illustrates the structure and the hierarchical relationship between the IAO, IAA and the SIRO.




**Project Managers / Other ICB Staff**
Organisations should ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements.

Requirements to ensure information security, confidentiality, and information quality should be identified and agreed prior to the design, development and/ or implementation of a new process or system. A Data Protection Impact Assessment should be completed and submitted for review.

Any use of personal identifiable information should be added to the Information Asset register and data flow mapped. Once the project is complete, the responsibility for reviewing and ensuring the use of personal identifiable information data flow maps are kept up to date must be handed over to the appropriate IAO.

**Data Security and Protection Toolkit (DSPT)**
The DSPT is an online system which allows NHS organisations and partners to self-assess against Department of Health and ISO Information Governance policies and standards.

The DSPT draws upon legal requirements such as the Data Protection Act and General Data Protection Regulation as well as best practice guidelines and presents them in one place as a set of information governance requirements. All NHS organisations are required

to submit a self-assessment against the DSPT data security standards annually. The IAO supports this assessment by providing evidence that forms a large part of the DSPT submission.

**Business Continuity Management**
A management process that enables an organisation:

- To identify those key services which, if interrupted for any reason, would have the greatest impact upon the community, the health economy and the organisation.
- To identify and reduce the risks and threats to ensure the continuation of these key services; and
- To develop plans which enable the organisation to recover services in the shortest possible time and maintain core services for the period it takes to fully recover critical systems.

**Business Continuity Plan**
A business continuity plan is a collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of a serious incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.

**Disaster Recovery Plan**
A disaster recovery plan is a documented process or set of procedures to protect and recover business IT infrastructure and systems in the event of a disaster. It describes the steps necessary to recover the system to a working state; the acceptable amount of data loss to the business; and how long the recovery is expected to take.

## 4. Roles and Responsibilities of an IAO

The IAO is responsible for ensuring the protection and preservation of the confidentiality, integrity, authenticity, availability, and reliability of information contained within their information assets.

A central part of the IAO role is understanding what information is held, what is added to and what is removed from the organisation's information asset register, how information is transferred, and who has access and why. That way IAOs will be able to understand what the risks are to their information assets and how these can be managed.

The IAO needs to provide assurances that information is shared only among authorised persons or organisations and that the information is reliable, complete and accurate. They need to ensure that information is held and transferred securely. They also have to provide assurance that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

If you delegate responsibility for ensuring actions are taken, you must make sure this is properly co-ordinated and that there are clear documented reporting chains that everybody understands.

IAOs are critical to ensuring information is properly handled. They are essentially the gatekeepers of information assets and advise the SIRO on practical policy steps.

## Summary of key aspects of the IAO role:

**An IAO needs to:**

- Ensure new information assets assigned to them have had a DPIA carried out and transfers of personal information identified are data flow mapped.
- Know what information assets are held/processed and for what purposes, including the legal basis for any data processing.
- Know what information the asset consists of and what information enters and leaves the asset and why.
- Understand how information is created, amended or added to over time.
- Be responsible for appropriate records management, including retention and disposal of information when no longer required.
- Know who has access and why and ensures access to the asset is audited.
- Ensure staff are appropriately trained and that only authorised staff have the required user access and making sure that staff are trained in using the asset and are aware of the records management procedures for that asset.
- Identify, understand, address, prioritise and review perceived risks to the owned asset and provide assurance to the SIRO on the security and use of assets.
- Have oversight of actions agreed to mitigate these risks.
- Protect the information held within the asset.
- Ensure all information assets are recorded in the Information Asset Register (IAR).
- Responsible for ensuring incidents are appropriately reported and investigated.

Some of these tasks will be delegated to and managed on a day-to-day basis by the Information Asset Administrator, but the IAO will always have overall responsibility.

There are a series of tools - detailed in the next few sections - available to assist the IAO in providing assurance. These will help the IAO in their role as well as provide the evidence required for the DSPT.

## 5. Training for IAOs

The IG team are able to provide support, advice and training to IAOs/ IAAs as and when required.

## 6. Information Asset Register (IAR)

Details of every information asset should be added to a central asset register file called an Information Asset Register (IAR). The purpose of the IAR is to identify the different types of information processed and stored by the organisation. It's an overview of all the information assets that exist within the organisation and is a useful tool for the SIRO and others for assessing risks and taking appropriate decisions.

This is also a key requirement of the DSPT.

It is important to ensure that the IAR is kept up to date and reviewed at least every six months. There must be a system in place to remind Information Asset Owners about this work and a structured reporting mechanism.

## 7. Data Flow Mapping (DFM)

Data Flow Mapping helps the organisation to understand what information it receives, where it is held and how it is transferred. The aim of data flow mapping is to:

- Identify assets collected and held by the organisation.
- Ensure that a legal basis for collection and processing has been identified and recorded.
- Ensure that appropriate secure storage has been established with access on a need-to-know basis.
- Ensure retention periods have been identified and recorded.
- Detail how the data is transferred.
- Ensure that any data that sent or received is secure in transit; and
- Understand the nature and justification of information flows to ensure the organisation is only sending and receiving information that it required.

IAOs will only need to map **regular** flows of information that contain **personal confidential data (PCD).** PCD relates to information about a person which would enable that person's identity to be established by one means or another. PCD can refer to any individual, not just patients so can include information about staff, contractors, visitors and members of the public.

**Bulk data flows** in particular should be mapped - It is essential to identify all instances where multiple records are being transferred out of each department, whether to other departments in the organisation or to other organisations. Bulk data is generally defined as person identifiable data relating to 21 or more individuals.

Data flows involving the transfer of fewer than 21 records should also be mapped with priority given to the impact of losing data. For example, the loss of a lower number of highly sensitive records is likely to have a greater impact than the loss of a large number of less sensitive records.

The mapping exercise relates to all data flows and may be by email, post/courier or portable electronic /removable media or system to system – this includes laptops, hand held devices, DVDs, CDs and USB sticks.

IAOs will need to think about:

- **Outbound flows:** What is sent to other departments in the organisation?
  What is sent outside of the organisation?

- **Inbound flows:** What is received from other departments in the organisation?
  What is received from outside of the organisation?
  What is collected from individuals, e.g. patients, staff, etc.

| We would suggest that the following means of transferring data should be mapped: | We advise you exclude the following from the data mapping exercise: |
|---|---|
| ✓ Email<br>✓ Post/ Courier - hard-copy or electronic media<br>✓ Text Message<br>✓ System to system transfers<br>✓ Transferred by staff | × Ad-hoc phone calls<br>× One-off transfers of information<br>× Transfers of anonymised information |

It is important to ensure that the DFM is kept up to date and reviewed at least every six months. There should be a system in place to ensure that this happens.

## 8. Risk Assessment

It is important that IAOs manage information related risks in relation to the information assets. A risk assessment must be completed for every identified information asset which holds personal information or is of key or critical importance to the organisation.

Any identified risks should be added to the departmental risk register. These should be reviewed and managed along with other risks. Where a risk has potential impact at an organisational level, consideration should be given to escalating the risk to the Corporate Risk Register.

**Examples of Risks to Manage**

- Inappropriate access to/ disclosure of personal data;
- Internal threats from staff or external parties;
- Information losses during transfer or periods of business change;
- Losses of immediate access to information/ continuity of access, i.e.: not being able to find, open, work with our information for a period of time;
- Poor information quality;
- Poor change management; and
- Failing to maximise the public benefits of information.

## 9. System Level Security Policy (SLSP)

It is a requirement of the DSPT that a System Level Security Statement is in place for key/critical systems (a collection of key/critical information assets). The purpose is to provide assurance that measures are in place to protect the data contained with the information asset.

The System Level Security Policy (SLSP) provides a system overview of the information asset i.e. what the system is used for. It also covers system security and the storage of information associated with the asset and how this information is processed.

A template for producing an SLSP is available (see Appendix A). In practice, most of the systems used by the ICB which would require an SLSP (for example, ESR or Systm1) would have an SLSP at national level.

## 10. Business/Service Continuity Plan

It is the responsibility of business continuity leads to ensure that business continuity plans (supported by risk management strategies, surge and escalation plans and winter plans) are in place for critical services. In some cases, the business continuity lead and IAO will be the same person but this is not always the case. It is important that IAOs and business continuity leads work collaboratively to assess the risks to service continuity and ensure that contingency plans are in place for critical and key information assets and that end users are familiar with these plans. Part of the risk assessment process may be to seek assurance from third party providers regarding the system support they can offer. Contingency plans for information assets might be stand-alone documents or form part of service-level business continuity plans for a department or directorate.

It is also useful to identify the time period that the department can function without the asset prior to activating the continuity arrangements. This time period may be as little as an hour or two, or may be a few days.

## 11. Disaster Recovery Plan

Disaster recovery plans clearly document the steps needed to recover a single IT system, or group of systems, after a disaster has occurred. They should describe a set of consistent actions to be taken before, during and after a disaster. The plan should clearly nominate who is able to invoke the plan and assign other responsibilities appropriately.

The plan will likely be drafted by the IT service responsible for the operational support of the information asset. The IAO should be aware of and ideally agree on the objectives within it. Specifically what data is backed up, how frequently and how long any recovery is expected to take. The frequency of backups may well determine the amount of data lost if a disaster occurs.

## 12. IT System Audit

Systems should have an audit facility in place. This audit should clearly show who has logged onto the system and the time and date that they have logged on. It should also show what changes have been made by users of the system and that only those users that should have access to the system do so.

There should also be documented confidentiality audit procedures that clearly set out responsibilities for monitoring and auditing access to confidential personal information held within the system.

**In addition to auditing systems IAOs are responsible for regularly reviewing access to shared folders, drives and files. To confirm who has access to a specific area this can be logged as a job via the IT Service Desk.**

The IAO has overall responsibility for auditing of the system and maintaining associated user accounts, but may delegate to the IAA to undertake this task. As a minimum this should include:

- Prompt removal of access rights by leavers / staff transferring to different positions
- Annual audit of access rights for any IT systems which the IAO is responsible for
- Participating in the annual audit of access to the network which will be co-ordinated centrally.

## 13. Data Quality

The DSPT stipulates that organisations have effective data quality controls in place and that records are maintained appropriately.

Having accurate, relevant information that is accessible at the appropriate times is essential to each and every health management or business decision and to the success of the service provided. With this in mind, it is essential that IAOs recognise the importance of DQ and their responsibilities in this area

Reference to Data Quality (DQ) is set out in the organisation's Records Management Policy but IAOs should be reminded of their responsibilities for DQ. The DQ requirements should also be documented as appropriate within any local records managements procedures and these should be made available to staff.

It is also important to ensure that the DQ is of a high standard in order to comply with the Data Protection Act 2018 in particular principle 4, 'accurate and up-to-date' and to satisfy the DQ requirements within the NHS Care Record Guarantee. The new legislation also contains a new principle of accountability for data controllers and processors and introduces new rights for data subjects, one of which is the right to have incorrect personal data amended.

The standards for good DQ are reflected in the criteria below. Data needs to be:

a) Complete (in terms of having been captured in full)
b) Accurate (the proximity of the data to the exact or true values)
c) Relevant (the degree to which the data meets current and potential user's needs)
d) Accessible (data must be retrievable in order to be used and in order to assess its quality)
e) Timely (recorded and available as soon after the event as possible);
f) Valid (within an agreed format which conforms to recognised national and local standards);
g) Defined (understood by all staff who need to know and reflected in procedural documents);
h) Appropriately sought (in terms of being collected or checked with the patient during a period of care);
i) Appropriately recorded (in both paper and electronic records); and
j) Processed in accordance with any existing data sharing agreement of data processing agreement.

As a commissioning organisation, the ICB has the responsibility of monitoring the DQ of the services it commissions. This will be carried out in a variety of ways according to the type of service and the data it collects. Examples include NHS number compliance,

pseudonymisation, compliance with new ISNs, Reference Cost Audits, DSPT DQ requirements.

IAOs should ensure that all staff working with information systems must be appropriately trained in DQ and the importance it commands for the management and provision of patient care.

## 14. Checklist for IAOs

This is a quick checklist of what needs to be done as an IAO and ensure they are properly managing their information assets:

***Ensure:***

- Data flow mapping is reviewed on a regular basis, quarterly for each information asset that processes PCD and your area of responsibility.

- Risk assessments for identified information asset(s) are undertaken on an on-going basis, preferably every six months. Risk assessments are completed by the IG team. When the Information Asset Register is reviewed, any risks that the IAO is aware of should be notified to the IG team as soon as possible;

- A System Level Security Policy is produced for every electronic information system that is key/ critical in importance (and no national / regional SLSP exists)

New assets are added to or old ones deleted from the Information Asset Register and to include any updates on any existing assets.

- Assistance is provided to the IG team in providing evidence to support the annual DSPT submission.

- DPIAs are completed, where required and follow organisational procedures.

- Data quality standards and associated responsibilities are met.

- Record Management policy, including retention and disposal etc.is adhered to.

- Audits of user accounts on a defined periodic basis are undertaken and that access rights for any leavers / staff transferring to different roles are removed on a timely basis. You can request a report from the IT Team, should you need to.

**APPENDIX A**

## SYSTEM LEVEL SECURITY POLICY TEMPLATE (SLSP)

### Information Asset Risk Assessment and System Level Security Policy

| | |
|---|---|
| Asset Name | |
| Asset type | |
| Data Controller | |
| Information Asset Owner | |
| Information Asset Administrator(s) | |
| Directorate/Division/Unit | |
| Business Criticality Rating (choose from pick list at end of this template - 1 to 5 ) | |
| Frequency of risk assessments | |
| IAA Role | |
| Authorised users (May be maintained in a separate list. Specify location of list, or attach a copy of it) | |
| What third party organisations have access to the asset (other than for maintenance/support) | |

| | |
|---|---|
| Purpose of third-party access | |
| Is there a contract/ISA in place for third party access referred to above | |
| If yes, to the above, who holds a copy of the contract | |
| Main business function (e.g. patient administration, finance) | |
| Asset scope (e.g. whole organisation, specified departments) | |
| Does the Asset hold PID/SPID<br>how will it be collected<br>how will it be stored | |
| What is the application and approval process for access to the asset | |
| Is end-user training/awareness provided | |
| If yes, who provides the training | |
| Is a training manual/guidance document available | |
| How are users made aware of procedures for reporting incidents<br>relating to the asset | |
| How frequently is access reviewed | |
| What controls are in place to deal with leavers/staff transfers | |
| Asset location | |

| | |
|---|---|
| Asset storage arrangements | |
| Origin of the asset (eg bought in, developed in house) | |
| Elements of the asset (eg SQL server, Windows server, appliance) | |
| Serial numbers for asset | |
| License numbers for asset | |
| License held by (eg IAO, ITC) | |
| Asset operating system | |
| Min patches required by OS | |
| Min patches required by asset | |
| Risk assessment period | |
| Disaster Recovery arrangements | |
| What business continuity plans are in place and who holds the plan (mandatory for criticality ratings for 3 and above) | |

| | |
|---|---|
| Maintenance/support contract in place | |
| approved by Trust | |
| start date | |
| renewal date | |
| company details | |
| primary contacts | |
| contact details | |
| Who holds the contract | |
| Does contract contain IG clauses | |

| | |
|---|---|
| Incorporated security measures | |
| Physical | |
| | |
| Logical | |
| Network | |
| Other | |

| | |
|---|---|
| Audit Capabilities | |
| Logins | |
| Administrator activities | |
| System changes | |
| | |
| Passwords | |
| min length | |
| complexity (e.g. alphanumeric) | |
| change period | |
| history (e.g. can reuse previous) | |

| | |
|---|---|
| Additional information | |

| | |
|---|---|
| Are there any information governance concerns regarding this asset. If so, what has been done/can be done to address them. | |

| | |
|---|---|
| Risk rating | 3 |

| | |
|---|---|
| Completed by: | |

| | |
|---|---|
| Date accepted by IAO | |

| | |
|---|---|
| Recommendations/action by IAO or IAA | |

| | |
|---|---|
| Date submitted to SIRO | |

| | |
|---|---|
| Review/repeat date: | |

| *For IG/SIRO use only* | |
|---|---|
| IG Team Comments/Recommendations | |
| Name of IG reviewer | |
| Date of IG review | |
| SIRO Recommendations | |
| Date accepted by SIRO | |
| SIRO name | |

**Business Criticality Ratings:**

| | | |
|---|---|---|
| Insignificant | No disruption to the organisation. Financial implications are negligible. Patient care is not adversely affected. | |
| Minor | The impact would threaten the efficiency of some aspects of the organisation. Some financial implications. The impact can be managed at a local service level. | |
| Moderate | Disruption to the organisation could be managed. Moderate financial implications. System outage affects more than one department/service. Patient care is significantly adversely affected. | |
| Major | Serious disruption to the organisation. High financial implications. Clinical risk is highly likely. System outage affects multiple departments/services. | |
| Catastrophic | System is crucial to the operation of the organisation. Significant financial implications. Clinical risk posed by system failure. System outage affects all departments/services. | |