NHS
Hull
Clinical Commissioning Group

NHS
East Riding of Yorkshire
Clinical Commissioning Group

The IAO/IAA Handbook

Key Guidance and Resources for Information Asset Owners & Information Asset Administrators

Version: 5.0
Date: August 2020

Table of Contents

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 CCG 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 provide assistance to IAOs. 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 i.e. 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.

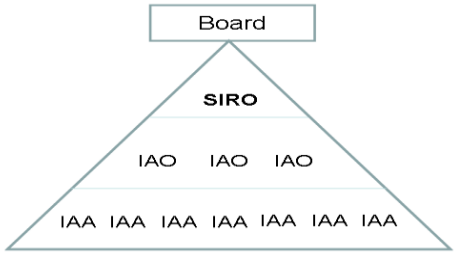
Information Asset Owner (IAO)
An IAO is an individual within an organisation that has been given formal responsibility for the security of an asset (or assets) in their particular work area.
They are responsible for the maintenance of the confidentiality of that asset, ensuring that access to the asset 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; and
e) Resolving system issues, including managing and auditing user accounts i.e. 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 CCG 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 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; and
- 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	× Ad-hoc phone calls
	× One-off transfers of information
✓ Post/ Courier - hard-copy or	× Transfers of anonymised

	electronic media	information
✓	Text Message	
✓	System to system transfers	
✓	Transferred by staff	

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 CCG 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 CCG network which will be co-ordinated centrally.

System Administrators:

Where an IAO is responsible for a system and maintaining the associated access rights to accounts they must complete and return the System Administrator Declaration Form at Appendix B as per the requirements of the DSPT. Completed forms should be returned to: Hayley.gillingwater@nhs.net

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 CCG 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 as a whole;

- 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; and

- 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.

INFORMATION ASSET OWNER / ADMINISTRATOR DECLARATION

I confirm that I have read and understood the Information Asset Owner and Administrator Handbook. I understand that it is my responsibility to raise any queries or concerns with my line manager or directly with the Information Governance team.

Signed:	
Name (Please PRINT):	
Date:	
Job Title:	

This completed form should be returned to your IG Lead / Specialist

APPENDIX A

SYSTEM LEVEL SECURITY POLICY TEMPLATE (SLSP)

System Details

System Name

System Owner

System Administrator

Overview

Describe its function and purpose; how it is used and accessed, where the information is stored as well as how any personal confidential data (PCD) is added to the system

Organisations, Departments and Services using the System

Other systems which are dependent on this one

System Supplier(s)

Support and Safeguards

System Maintained By (list all responsibilities)

Renewal Dates of Any External Support Contracts

Supported Hours for System

Person Responsible for System Security

System is accessible From: (The Internet/ N3 / Local networks)

Caldicott Guardian

Does the system hold patient records? YES / NO

Is this system classed as a clinical system? YES / NO

Does the system use the NHS number as an identifier? YES / NO

If the system holds PCD, please detail:

Anonymisation and Pseudonymisation Measures in Place

Security Safeguards (please add any additional measures)

NAME	ANSWER	NAME	ANSWER
Secure Room / Cabinet	Yes/No	Record Tracking	Yes/No
Security Alarms		Records Physically Sealed During Transport	
CCTV		Strong Passwords or Smartcards used	
Stored Data is Encrypted		Strictly Controlled User Access Rights	
Antivirus in Place		User Activity Audited	
Operating System Updated Regularly		Strict Printing control	
Network Firewalls		Bulk Extracts of PID prevented or restricted	
Servers in Restricted Network Area (DMZ)		System Alerts monitored	
Network Traffic Encrypted		Independent Security Testing	

Disaster Recovery Plan (name and location)

Business Continuity Plan (name and location)

Network Connectivity Diagrams (simplified overview only)

The system will be risk assessed according to standard processes and procedures.

Process for Requesting Access

Sponsor required for new users or additional permissions
(e.g. line manager, IAO, director)

Link to user guides/ training documentation

Person responsible for regularly reviewing user accounts and permissions
(Minimum of every 6 months)

Passwords Can Be Reset Using the Following Processes

Temporary and Shared Accounts (detail approach to issuing, if their use is allowed)

Additional Controls and 3rd Party Access

System Accounts (e.g. administrator, standard, read-only)

System Account Type	Permissions Granted by Account Type

Password / Access Security Settings

Security Setting Name	Detail
Minimum Password Length	
Complex Password Required	
Password Length	
Forced Password Changes (in days)	
Password Re-use Allowed	
Common Passwords Blocked	
Number of Failed Logins Allowed	
Session Timeout (in mins)	
Access Limited to Specific Hours	
Access Limited to Specific PCs/ Devices/ IP Ranges	
Number of Simultaneous Logins Allowed to One Account	
More Stringent Policies in Place for Power/ Admin Users	

Third Party Access

Organization or Individuals Name	Reasons for Access	Access Agreement

Appendix B

System Administrator Declaration Form.

Expectations for the Protection of Personal and Confidential Information

As a System Administrator by the nature of your role you have greater access rights in comparison to a normal system user. Normal user access can be restricted to role and is usually limited to what those users need to do or perform as part of their job role, therefore protecting themselves and the organisation.

In your System Administrator role the additional access privileges you are granted to fulfil system administration tasks, place you in a position of additional responsibility and trust. In particular this is the case where the information held on the system is of a confidential nature such as staff and patient identifiable information and commercially sensitive information.

The Data Security and Protection Toolkit sets out a mandatory requirement that System Administrators of systems holding personal and confidential information, agree to ensure they follow high standards of use of the system(s) they administrate. The reason for this is because System Administrator roles are becoming more and more important as far more information than ever is held electronically and as the threat from cyber security attack grows.

As a System Administrator your responsibilities may include some or all of the following (*list not exclusive of all responsibilities of a System Administrator*):

- Adding users and permissions
- De-activating and removing users as individuals leave the CCG, change role or take special leave
- Carrying out regular audit of user accounts (guidance on which can be found on page 4 of this document)
- Configuring system security such as password complexity, number of failed log in attempts and system timeout
- Training users in the proper use of the system
- Facilitating the implementation of upgrades and patches by the system provider
- Trouble shooting and problem solving system issues as they occur. Liaising with the system supplier
- Running and reviewing system audit trails as routine or on request
- Supporting investigation of any misuse of the system.

See over page

Expectations of the System Administrator Role

- You keep your System Administrator log in details private and do not share them with others.
- If you suspect your log in details have been compromised you report this immediately to the system Information Asset Owner and the System Supplier as well as reporting as an incident through the CCG incident reporting procedure.

- You are aware of the need to protect the privacy of personal and confidential information that is held on the system, in line with the requirements of data protection legislation and the policies of the CCG.
- You take steps to ensure the system security settings are configured in line with the policies of the CCG, seeking the advice of the Information Governance Team and Data Protection Officer as required.
- You only view what you need to, to administer the system and do not browse the system and records unnecessarily
- You do not disclose personal and confidential information which you may incidentally access as part of your System Administrator role
- You act with respect in relation to users reasonable expectations of privacy ensuring you do not unnecessarily browse user log files and audit trail reports without a specific remit or request to do this
- You do not amend records inappropriately.

Please provide the following information about the system:

Name of System	
Name of Information Asset Owner	

Does each individual have their own login and password? *(please tick) i.e.no accounts are shared and no generic accounts are used*	**Yes**	
	No	

Is the password criteria set at 'high strength'? *i.e. passwords require numbers, letters (upper and lower case) and punctuation*	**Yes**	
	No	

Does the system support Role Based Access? *(please tick) ie gives staff access rights only to the information staff need to do their jobs*	**Yes**	
	No	

How is user access monitored? *If user access is not monitored please note this also.*

Do administrators have separate login credentials to carry out "administrator role" tasks separately to "basic user" tasks?	**Yes**	
	No	

See over page

Provide details of what roles exist within the system and the numbers of staff against each role. Example overleaf. Add more rows as required.		
Role	***System Access Functionality***	***Number of accounts***

Please check

☐ I confirm that I have read and fully understand the expectations and behaviours required of me in my role as a System Administrator.

☐ I confirm that an audit of user accounts has been carried out for the system.

☐ Users who no longer require access have been removed from the system.

☐ Users' access levels have been appropriately reconfirmed/ amended according to role.

If I have any questions or queries I will speak to a member of the Information Governance Team.

Information Asset Owner Name and Signature:	
System Administrator Name:	
Job Title:	
Signature:	**Date:**

See over page

Acknowledgements:
NHS Digital Data Security and Protection Toolkit 2020, Big Picture Guide Standard 4

Example

Example of system role based access		
Role	***System Access Functionality***	***Number of accounts***
Admin	Ability to amend, delete and create new tables and look up fields	2
General user	Ability to add, amend and delete own created records and view others	50
Super user	Ability to add, amend and delete own created records, amend and view others	3
View user	Ability to view all records	8

Backup user	Technical account used to archive the systems database	1

Audit of User Accounts Guidance	
Step 1: Generate a list of current users	• Generate a list of individuals who currently have access to the system, and each individual's access level. • You should be able to do this from the system itself, but if not you may need to contact the supplier.

Step 2: Review current user access	• Check the list of current users against staff that have:
	  ○ left the organisation,
	  ○ Changed to a role where access is no longer required.
	• Remove anyone with unauthorised access to the system.

Step 3: Review of users access level	• Once an up to date list of users is established, check users access levels are correct.
	• Consider:
	  ○ What they need to do in the system e.g. add/remove users, input data.
	  ○ Does their current access allow more/less access than is required?
	  ○ What is the lowest level of access that will allow them to do what they are required to do?
	• Adjust individual access levels as appropriate.
	• Ensure this is undertaken in collaboration with the IAO and individual users' of the system(s).

Step 4: Completion	• If you have any queries about undertaking the audit of user accounts, seek advice from the IG Team before you start. • Return completed declaration to Hayley.gillingwater@nhs.net