NHS
Urgent Care 24

Information Asset Policy

Version	1.2
Location	Policy Folder – Information Governance
Approving Committee:	Executive
Date Ratified:	August 2011
Reference Number:	UC24POL33
Name/Department of originator/individual:	Stephen Mather
Name/Title of responsible committee/individual:	Service Delivery Manager
Date issued:	August 2011
Review date:	January 2017
Target audience:	Information Asset Owners, Information Asset Administrators

Version	**Date**	**Control Reason**
1.0	01/11/2012	Policy reviewed by SM.
1.1	01/02/2015	Reviewed in line with annual information governance submission.
1.2	27/01/2016	Reviewed in line with annual information governance submission.

CONTENTS

Appendices

1.0 PURPOSE

The purpose for this document is to provide a mechanism to achieve and maintain appropriate protection of the organisations information assets. All major information assets must be identified and have a responsible owner and maintenance responsibilities assigned.

This document has been implemented to provide guidance on:-

- How to identify an information asset
- Populating and maintaining the information asset register
- Treating and managing risk for information assets
- Identifying the key roles for information assets
- Disposing and archiving an information asset
- Managing an information asset
- Auditing an information asset

This policy should be read in conjunction with the following policies: Information Security Policy (UC24POL6), Risk Management Strategy (UC24POL4), Records Management and Strategy (UC24POL3), Information Disposal Policy (UC24POL45)

2.0 SCOPE

This policy applies in particular to employees of Urgent Care 24 and outlines the procedure adhered to in this policy. This document is set out to define the procedures for creating, updating and disposing of local information assets. It also includes instructions in relation to the annual audit of said assets.

This document is primarily intended for:

- Information Owners
- Information Managers
- Information Asset Administrators
- Data Managers
- Information Users.

3.0 BACKGROUND

The Information Governance Toolkit is made up of Information Governance related national requirements which are set out by Connecting for Health.
Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of Urgent Care 24 services and resources.

The toolkit plays a key part in clinical governance, service planning and performance management and decision-making. It is therefore of paramount importance that information is effectively managed in line with current Urgent Care 24 policies and standard operating procedures which can be found on the Urgent Care 24 Intranet. It is also important that management accountability is identified to provide a robust Information Governance framework to support the organisation. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of Urgent Care 24 services and resources.

- To support the provision of high quality care by promoting the effective and appropriate use of information.
- To encourage employees to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide employees with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

4.0 DEFINITION OF AN INFORMATION ASSET

Critical Information Assets are those that are central to the efficient running of departments within Urgent Care 24 for example, patient information and finance. Non computerised systems holding information must be recorded on the asset register detailing relevant file identifications and storage locations.

There are six main categories of information assets:

- **Information** – this includes databases, system documentation and procedures, archive media and data
- **Software** – this includes application programmes, systems, development tools and utilities
- **Physical** – this includes infrastructure, equipment, furniture and accommodation used for data processing
- **Services** – including computing and communications, heating, lighting, power, air conditioning used for data processing
- **People** – including qualifications, skills and experience in the use of information systems
- **Other** – for example the reputation and image of Urgent care 24

An information asset is defined within Urgent Care 24 as:

"An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a

recognised agency requirement. Data or information that is referenced by an agency, but which is not intended to become a source of reference for multiple business functions is not considered to be an information asset of the agency"

Table of information asset types with examples of each

Asset type – do the following information stores exist in your organisation?	Examples of assets
1. Organisation paper file records	• Assets register • Paper Files
2. Electronic record management systems or shared drive	• Electronic document management system (EDMS) • Shared network drive
3. Ad hoc filed material	• Newspaper clippings, posters and/or pamphlets put in individual bottom drawers or book cases 'in case they are useful'
4. Collections of published material	• Books • Published NHS documents • Consultant's reports
5. Unpublished literature (also termed 'grey literature')	• 'Grey literature' is material such as working documents or reports that have not been formally published or made publicly available
6. Electronic records	• Emails • Your organisation's shared drives • Personal drives
7. Electronic records continued	• Photo collections • DVDs and Videos • CD ROMs • Audio recordings • Medical Records
8. Functionality for searching electronic records	• Search facilities for shared drives • Naming conventions for files
9. Metadata	• 'Metadata' is information about information, for example library index cards
10. Your organisation's website and Intranet including its content	• Policies • SOPs • Accessibility • Search capability
11. Data sets and collections	• Data collected from analysts • Data sets from consultants work
12. Decision making tools	• Decision Support Tool software
13. Learning software	• Mind mapping software or other specific learning applications

Asset type – do the following information stores exist in your organisation?	Examples of assets
14. Governance arrangements	List of people within your organisation responsible for: • Records management • Clinical Governance • Information Governance
15. Lost corporate information	• Important databases, websites, or personal collections that the organisation has lost and which may need to be regained or recreated
16. Information transfer	• Induction processes for new staff
17. Disaster and risk management planning	• Disaster and risk management plans
18. Unique sources of information	• Specialised information resources unique to the organisation which may be held by the organisation or other agencies such as NHS bodies

5.0 MANAGING INFORMATION ASSETS

Owners and Custodians

The roles and responsibilities of information asset owners should be explicitly defined and understood throughout the organisation. Owners will nominate custodians known as information asset administrators (IAA) to implement security controls that are commensurate with the security needs of an information asset.

The job of planning and managing security is the responsibility of the information asset owners. The information asset owner and information asset administrator concepts enable complex situations for managing the security of an information asset.

The information asset owner (IAO) and information asset administrator can be the same person however the difference between the roles is determined by the information asset owner and the responsibilities they delegate to the information asset administrator. The information asset administrator will tend to be responsible for the routine management of the information asset.

6.0 ASSET REGISTER

Information assets must be documented in the Urgent Care 24 information asset register, without this list it would be impossible to implement the required controls across Urgent Care 24. The asset register will be held by the Service Manager with responsibility for Information Governance on behalf of the Senior Information Risk Officer. The asset register (IAR) is reviewed on a regular basis to ensure that the information is accurate and concurrent with the actual assets that are currently operated within Urgent Care 24. A review will also occur after any major organisational change. These changes will include incidences such as the implementation of a new system or the redundancy of an existing system. The Service Manager with responsibility for Information Governance in cooperation with information asset owners will record all of Urgent Care 24's Information assets in Urgent Care 24's Information asset register.

This register will record and identify the following information surrounding the asset:

- Identifies the information asset owner and information asset administrators for the asset
- Does the Information Asset have a system level security policy
- Has the Information Asset undertaken a Business Continuity Plan
- Identifies Data Flows and Information Mapping
- Risk Assessment in line with the Urgent Care 24 Risk Management policy undertaken on the Information Asset
- How the Asset is Stored and in what format it is used
- Is the Information Asset a ***Critical or Non Critical*** asset

Critical information assets must be implemented using an eight step process as show in (**Appendix four**)

7.0 CHANGING AN IAO OR IAA

Changes to an information asset owner or administrator must be notified to the Senior Information Risk Officer.

Changes should be notified at the time they become known to enable the Information Governance lead to be aware of the handover of assets and registers and provide advice and assistance if needed.

8.0 KEY ROLES AND PROCESS FOR INFORMATION ASSETS

There are four roles required to ensure structured management arrangements for information risk. These include:

Role	Responsibility	SMHP Role
Accounting Officer	The *Accounting Officer* has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks must be handled in a similar manner to other major	Chief Executive

	risks such as financial, legal, and reputation risks.	
SIRO	The *Senior Information Risk Owner* is an executive who is familiar with and takes ownership of the organisation's information risk policy and acts as an advocate for information risk on the Board	Director Of Service Delivery and Operational Performance
IAO	Information Asset Owners must be a member of staff who is senior enough to make decisions concerning the asset at the highest level. The owner can assign day to day responsibility for each information asset to an administrator or manager, which must be formalised in job descriptions. Their role is also to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.	Directors / Line Managers / (See Information Asset Register)
IAA	Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents / threats, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date	System Administrators/ Super Users

9.0 DISPOSAL AND ARCHIVING OF INFORMATION ASSETS

Information assets and their components may need to be replaced or destroyed because they have either become surplus to requirement or reached their operational life, and as such they require to be safely and securely disposed or archived.

The decision to destroy or archive an information asset or the component should be explicitly outlined in the system level security policy. This section explains how to archive or dispose of information assets in line with Urgent Care 24's information disposal policy (UC24POL45).

Disposing of an Information Asset (**see fig1**)

- Information Asset end of life has been determined
- Information Asset Owner will trigger the process
- The type of Information Asset is determined
- Information Asset Owner will notify IM&T and the Senior Information Risk Officer if the Information Asset is electronic based
- Authorised means of disposal to be used
- Certification received for destruction
- Information Asset Register updated

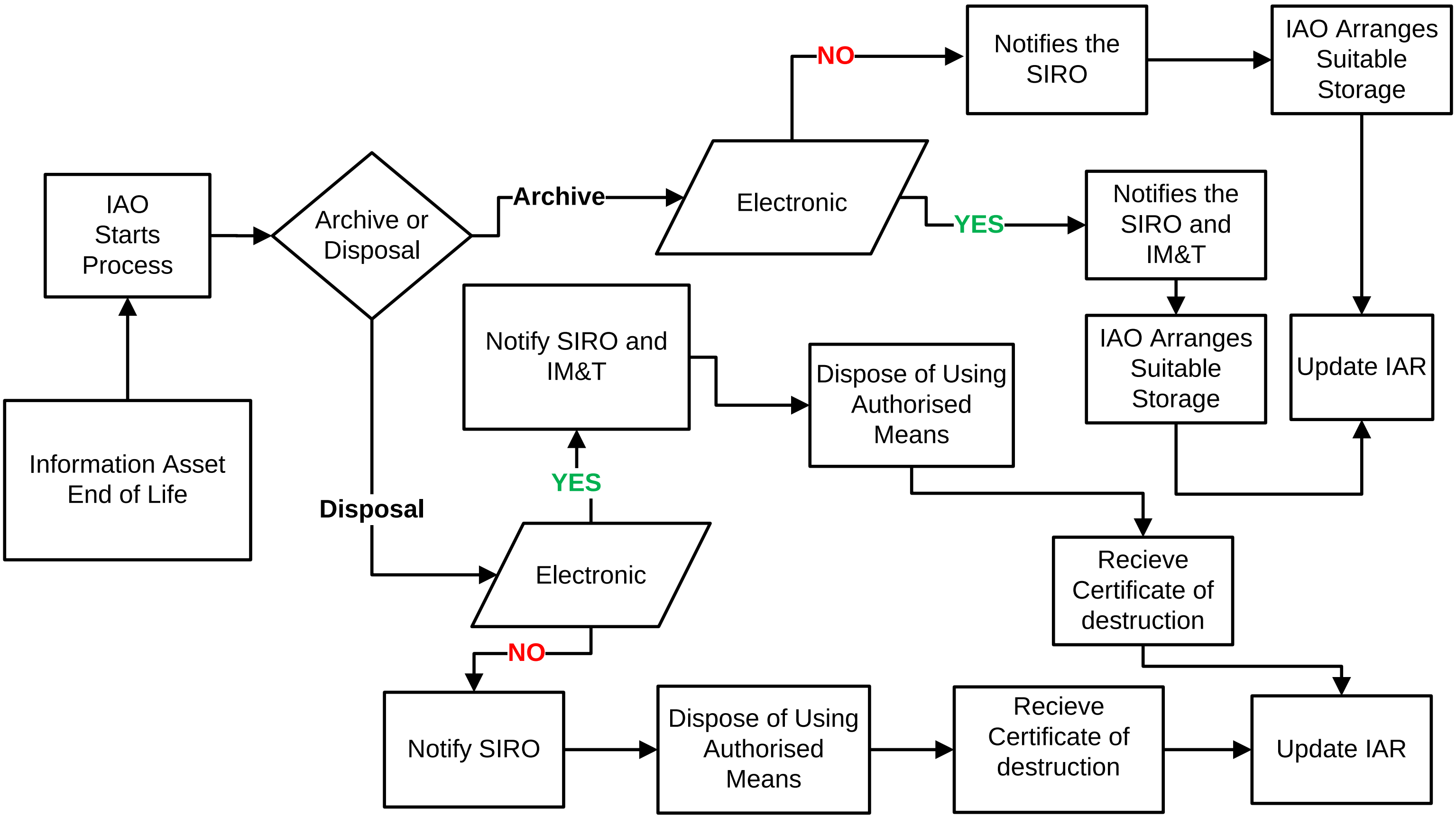
Before disposal can be implemented then an information asset disposal form (**Appendix five**) must be completed and signed off by authorised members of staff. Note: Only the Information Asset Owner can submit an Information Asset Disposal form.

Archiving an Information Asset (**see fig 1**)

Disposal of an information asset will be implemented using the following guidelines:-

- Information Asset end of life has been determined
- Information Asset Owner will trigger the process
- Information Asset type is determined
- Information Asset Owner will notify the Senior Information Risk officer if the Information Asset is **non** electronic based
- Information Asset Owner will arrange suitable storage for the Information Asset
- Information Asset Register updated

Fig 1- Archiving and Disposal of an Information Asset


Information Asset End of Life
IAO Starts Process
Archive or Disposal
Archive
Electronic
NO
Notifies the SIRO
IAO Arranges Suitable Storage
YES
Notifies the SIRO and IM&T
IAO Arranges Suitable Storage
Update IAR
Disposal
Electronic
YES
Notify SIRO and IM&T
Dispose of Using Authorised Means
Recieve Certificate of destruction
NO
Notify SIRO
Dispose of Using Authorised Means
Recieve Certificate of destruction
Update IAR

10.0 INFORMATION FLOW MAPPING

All critical information assets require an information mapping exercise to be carried out to ensure that all data flows of information in and out of the asset have been identified. Information mapping will help to identify any potential risks and issues associated with the asset. The following stage is to develop a plan to mitigate any of the identified risks using the risk management process adopted within the Urgent Care 24 risk management process.

Information mapping should be identified and risk assessed for the Information Asset. Information mapping should be carried out using the mapping tool on the Information Governance toolkit.

- For guidance on mapping information see the attached document below:

NHSCFH Info Map
Tool Guidance Vers 2-

11.0 RISK MANAGEMENT OF AN INFORMATION ASSET

Achieving long-term success requires that Urgent Care 24 makes efficient and effective decisions when deploying limited resources (personnel, time, and money).

The identification of critical Information Assets is the first step in performing an information security risk assessment. Collectively, these assets define what is important to the organisation and must be protected. A critical information asset is an asset that is essential to the organisation’s ability to achieve its goals and objectives.

Once information asset profiles have been completed for critical information assets, the organisation can begin the process of identifying risks to those assets and planning strategies to mitigate the risks. A typical information security risk assessment consists of several major activities:

- characterising risks (from vulnerabilities and threats)
- determining the consequences to the organisation if these risks are realised
- evaluating, categorising, and prioritising which risks need to be mitigated
- developing corresponding mitigation strategies and plans

Typically an information security risk assessment considers the following.

- The environment that the information asset is stored/located
- The methods of storage
- Access including accidental
- Limitations in the information assets design

This list is not exhaustive

Another important benefit of identifying key containers for assessment is that it ensures that internal and external risks to an information asset are considered. Information assets are often transported across organisational boundaries, yet traditional risk assessments may focus on vulnerabilities and threats that affect only the key containers that are under the organisations direct control.

12.0 ANNUAL AUDIT OF ASSET REGISTERS

To ensure the Asset Register remains current, accurate and complete it will be subject to an annual audit and spot checks. Information Asset Owners should undertake regular reviews to manage the information risks associated with their relevant assets.

Appendix one

Key Responsibilities

Title: Senior Information Risk Owner (SIRO)

Purpose of Role:

The Senior Information Risk Officer will implement and lead Urgent Care 24’s Information Governance (IG) risk assessment and management processes within the Organisation and advises the board on the effectiveness of information risk management across the Organisation.

Specific Responsibilities:

The key roles of the SIRO are:

- Understand how strategic business goals of Urgent Care 24 may be impacted by information risks
- Acts as an advocate for information risk on the Board
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment
- Review and agree actions in respect of identified information risk
- Ensure that Urgent Care 24’s approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Ensure the board is adequately briefed on information risk issues
- The SIRO will be required to undertake strategic information risk management training at least annually

Appendix two

Job Description

Title: Information Asset Owner (IAO)

Purpose of Role:

Information Asset Owners are senior individuals involved in running the relevant business.

The IAOs role is to:

- Understand and address risks to the information they ‘own’
- Provide assurance to the SIRO on the security and use of these assets

Specific Responsibilities:

- Maintains understanding of ‘owned assets and how they are used
- Approves and minimises information transfers while achieving business purposes
- Approves and oversees the disposal mechanisms for information of the asset when no longer needed
- Knows what information the asset holds and who has access to update the system
- Takes visible steps to ensure compliance to the organisation Information Governance strategy and action plan
- Undertakes quarterly reviews on the information risk associated with the asset
- Undertakes and addresses risks to the asset and provides assurances to the SIRO
- Knows who has access and why, and ensures their use is monitored and complain with policy
- Receives, logs and controls requests from other for access
- Ensures that changes to the system are put through a formal ‘Request for Change’ process with relevant Equality Impact assessment and Privacy Impact Assessment completed.

Appendix three

Job Description

Title: Information Asset Administrator (IAA)

Purpose of Role:

Information Asset Administrators will provide support to their IAO to:

- Maintenance of Information Asset Registers
- Ensure compliance with data sharing agreements within the local area
- Ensure information handling procedures are fit for purpose and properly applied
- Under the direction of the IAO, ensure that personal information is not lawfully exploited
- Recognise new information handling requirements and the relevant IAO is consulted over appropriate procedures
- Recognise potential or actual security incidents and consulting the IAO
- Report to the relevant IAO on the current state of asset
- Act as a first port of call for local managers and staff seeking advice on the handling of information
- Under the direction of the relevant IAO ensure that information is securely destroyed when there is no further requirement for it (Refer to Urgent Care 24’s Records management Policy for further guidance)

Appendix four

Critical Information Asset Check List Process:

No	Item/Process	SIRO	IAO	IAA
1	Register Asset In Information Asset Database	□	□	□
2	SLSP (System Level Security Policy) if applicable	□	□	□
3	Information Mapping Exercise undertaken on the IGT Toolkit	□	□	□
4	Risk Assessment of Information Transfers	□	□	□
5	Action Plan Produced Against Identified Risks documented in the Risk Register	□	□	□
6	Change Request Process initiated	□	□	□
7	Business Continuity Plan implemented for the asset if applicable	□	□	□
8	Training of Business Continuity to Staff if applicable	□	□	□

NHS
Urgent Care 24

Appendix five

Information Asset Disposal/Archive Form

YOU’RE DETAILS

DEPARTMENT AND LOCATION	
CONTACT PERSON FOR ENQUIRIES (PRINT NAME)	
TELEPHONE CONTACT NO	
FULL EMAIL ADDRESS	

DESCRIPTION OF ITEMS

ASSET REGISTER NUMBER	
ASSET TYPE	
DESCRIPTION	
MANUFACTURER	
☐ DISPOSAL ☐ ARCHIVE	
REASON FOR DISPOSAL/ARCHIVE	
SELECT DISPOSAL METHOD	

PROPOSED BY		**SIGNATURE**		**DATE**	
AUTHORISED BY		**SIGNATURE**		**DATE**	

Appendix six

Urgent Care 24
Information Asset Audit Checklist

Audit Undertaken by:	
Date of Audit:	
Asset Number	

Routine Staff Monitoring & Compliance Spot Checks IG

Security measures to the Asset are adequate and in working order	□
Access to the Asset is in line with the Information Asset Register	□
Information is in line with the Records Management policy	□
Risk Assessments have been undertaken and reviewed for the Asset	□

Notes:

Appendix seven

Information Asset Risk Assessment Form

Information Asset		**Information Owner**	
Description of Information			

Description of Risk	**Impact**		**Likelihood**		**Impact * Likelihood**		**Action to reduce risk**	**Responsibility**
	Gross	Net	Gross	Net	Gross	Net		
