NHS
Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM5
Issue number: 4.01

Information Asset Register Policy

Lead executive	Medical Director & Caldicott Guardian
Authors details	Trust Records & Information Governance Manager/Data Protection Officer

Type of document	Policy
Target audience	All CWP staff
Document purpose	This policy sets out the purpose of the Trust information asset register and the responsibilities of the SIRO, Information Asset Owners, Information Asset Administrators and all Trust staff

Approving meeting	Information Governance & Data Protection Sub-Committee	23/05/2019
Implementation date	June 2019	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM1	ICT Acceptable Usage Policy
IM7	Confidentiality Policy
IM10	Information Governance Policy
GR1	Incident Reporting Policy
FR1	Integrated Governance Strategy

Document change history	
What is different?	1. Updated references to Records & Information Systems Group to Information Governance & Data Protection Sub Committee 2. Updated references to Information Governance Toolkit to Data Security and Protection Toolkit 3. Updated list of top critical systems 4. Replaced reference to gerenal managers to heads of operations 5. Page 17 removed reference to EEA and replaced with UK
Appendices / electronic forms	Not applicable
What is the impact of change?	Not applicable

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	None

Financial resource	None

implications	

External references
N/A

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
Not applicable		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	N/A	

Contents

Quick reference flowchart for Information Asset Owners
For quick reference the guide below is a summary of actions required.

Training
Information asset owners (IAO's), information asset administrators (IAA's) and the SIRO must all undertake the appropriate e-learning packages

↓

Data flow mapping
IAO's/IAA's will undertake a data flow mapping exercise on an annual basis and include this in the annual risk report to the SIRO

↓

Information asset register
IAO's/IAA's will check the information asset register on an annual basis

↓

Annual risk report to SIRO
IAO's will undertake an annual risk report to the SIRO to provide assurance of risk assessment and monitoring

↓

Monitoring
Risks will be recorded with the appropriate risk register and all risk/associated actions will be reviewed at regular intervals

↓

Information Governance & Data Protection Sub Committee (IG & DP SC)
IG & DP SC will review data flow mapping/information asset register/IAO's annual reports to the SIRO

1. Introduction

This policy sets out Cheshire and Wirral Partnership NHS Foundation Trust's (CWP) Information Asset Register Policy. The policy outlines how the Trust undertakes risk management of key Information Assets. Information Assets (IA) are valuable to the clinical and business functions of the organisation. Regular reviews of implemented information security arrangements are an essential feature of an organisation's risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

1.1 Objectives

The objectives of this policy are to:

- Protect patient and staff information;
- Protect the Trust's corporate records;
- Protect the systems and environments where information is stored;
- Protect the processes by which information is accessed;
- Provide a consistent risk management framework;
- Encourage pro-active rather than re-active information risk management.
- To ensure compliance with legislative and information governance assurance framework.

1.2 What are Information Assets (IA)?

There are various categories of Information Assets including:

- **Databases -** Current and archived;
- **Paper records -** Current and archived;
- **Software -** Applications, programs, systems development tools and utilities;
- **Physical -** Infrastructure, equipment, furniture and accommodation used for data processing;
- **Services -** Computing and communications, heating, lighting, power, air-conditioning used for data processing;
- **People -** Qualifications, skills and experience;
- **Policies -** Procedures, guidance and training;
- **Intangibles -** Public confidence in the organisation's compliance with Data Protection Legislation and NHS Code of Confidentiality.

1.3 What is the information asset register?

An information asset register is a document listing all the Trust's assets which hold information and which records assessed risks. Appendix 2 illustrates the format of the information asset register. The Senior Information Risk Owner (SIRO) will oversee the Trust's information asset register to ensure it is complete and robust. The ICT department have a separate network monitoring tool which is a real time asset register of ICT hardware.

There are a number of systems/assets within the Trust which are regarded as the top critical systems/assets. The following systems/assets have been approved by the SIRO as the top critical systems/assets:

- Electronic patient record systems
- PCMIs
- Adastra
- Datix
- Health Roster
- C-Scan
- Printing/Scanner
- Door Security
- Building Management System
- Micad
- Intranet
- Neo Post

- Docman

Approved business continuity plans must be in place for all critical information systems/assets. Business continuity plans, and system specific procedures and control measures are regularly reviewed, and where necessary tested, to assess their ability to meet their business objectives. See appendix 1 for business continuity plan template. The top critical systems/assets with associated business continuity plans have been included in the information asset register. The information asset register has been reviewed by the Information Governance & Data Protection Sub Committee and is available on the Trust's intranet.

2. Duties and Responsibilities

2.1 Senior Information Risk Owner (SIRO)

The SIRO is responsible for coordinating the information standards within the Trust through the membership and activities of the Information Governance & Data Protection Sub Committee (**see** Appendix 3). The SIRO ensures the organisation is developing its approach for ensuring recovery and continuity in the face of disaster or other major incident or business disruption.

2.2 Information Asset Owners (IAO)

It is important that *ownership* of each Information Asset is linked to a post rather than a named individual. Within Cheshire & Wirral Partnership NHS Foundation Trust Information Asset Owners are heads of operations and heads of departments. This ensures responsibility for each asset is passed on when IAOs leave or changes roles.

Information asset owners are required to:

- undertake a data flow mapping exercise annually as part of the risk/assessment report for the SIRO (this may be delegated to the IAA)
- Review information asset register (this may be delegated to the IAA);
- IAO's will undertake and provide a risk assessment/report for the SIRO on an annual basis (risk report for SIRO appendix 6)

2.3 Information Asset Administrators (IAA)

Information Asset Owners may nominate key functions to IAAs to assist the IAO in the operational management of an asset (see appendix 5).

2.4 All staff

All staff have a contractual obligation to ensure confidential and Person Identifiable Data is secure all at times. The framework for this obligation is defined in:

- The Code of Conduct for Employees in Respect of Confidentiality;
- The NHS Code of Practice on Confidentiality 2003;
- General Data Protection Regulation 2016/Data Protection Act 2018;
- The Caldicott principles;
- Trust Information Governance Policies.

3. Training

Training to be undertaken as e-learning for key personnel with training appropriate to the organisational needs and individual's roles and responsibilities.

4. Information incident reporting

All incidents of confidential and or person identifiable data breaches must be recorded on the Trust's reporting system as per the Trust's Incident reporting policy Serious incidents must be reported to the Trust Records & Information Governance Manager/Data Protection Officer to assess whether the incident requires external reporting. A checklist for Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation may be found on the intranet:Incident Reporting Guidelines

5. Monitoring

This policy will be monitored by the Information Governance & Data Protection Sub Committee against the data security and protection toolkit requirements and:

- Receive and review information risk reports from IAO;
- Review information governance related incident reports;
- Review the information asset register.

Once identified, information security risks need to be managed on a formal basis. Risks should be recorded within the appropriate risk register and action plans should be in place to demonstrate effective management of the risks. The risk register and all associated actions should be reviewed at regular intervals.

6. Further guidance

Further guidance on the arrangements for information risk management can be accessed via nhs digital's Asset Management Good Practice Guide.

NHS
Cheshire and Wirral Partnership
NHS Foundation Trust

Appendix 1 Business Continuity Plan (BCP) for Critical Asset Template

Name of Critical Asset	

Version	
Ratified by	
Date ratified	
Author(s)	
Responsible committee / officers	
Date issue	
Review date	
Intended audience	
Impact assessed	
Emergency Planning Lead	

Further information about this document

Document name	
Author(s) - Contact(s) for further information about this document	
This document should be read in conjunction with	CWP Major Incident Plan CWP Strategic Business Continuity Plan Individual business impact analysis

Version Control

Version History		
Version Number	Reviewing Committee / Officer	Date
	General Manager / Members of the Emergency Planning Sub- Committee	

Introduction

Business continuity – Critical Assets

A system of such importance to the organisation that it's unavailability to access will have a very serious impact to the delivery of CWP services.

This plan was completed by

Print name			
Position			
Signature			
Date		Ext	

This plan was reviewed annually by

Print name			
Position			
Signature			
Date		Ext	

Name of Critical Asset
Critical Asset Owner/ Contact details Owner Name:
Email Address:
Contact Number:
How will you know if the critical asset is unavailable?
How will you know how long the critical asset will be unavailable for?
What is the escalation process for a resolution?
What is the communications strategy for users?
What are the core activities if the service is not restored within 8 hours
What are the core activities if the service is not restored within 24 hours
What are the core activities if the service is not restored within 72 hours

Appendix 2 - Format of information asset register

						NHS IG security requirements	NHS IG Risk Assessment	
Date	**Description**	**Information owner / Data controller**	**Information type**	**Protective Classification (confidential or general)**	**Physical Location**	**Access control**	**Back up**	**Disaster Recovery Plan**

Glossary of terms

Hardware / physical	Equipment, furniture and accommodation
Removable media	Floppy disks, Data CDs or DVDs, USB flash memory sticks or pens, Zip drives and portable hard drives
Software	Applications, system, development tools and utilities
Services:	Computing and communications, heating, lighting, power, air-conditioning
Information	Databases, system documents and procedures, archived information etc.
Asset type	Enter the asset type e.g. PC, laptop, PDA, server etc.
Authorised purposes	Enter the usages that have been authorised / approved
Cost	Enter the cost or anticipated replacement cost of the asset or service
Date	This is the date of actual entry into the inventory
Date De-commissioned	Enter the date that the asset was taken out of use
Helpdesk support contact point	Enter the support contact details for the service
Information owner / data controller	This is the person responsible for control and management of information assets
Information type	Enter what type the information is e.g. patient database, spreadsheet, paper etc
Location (systems)	Enter the physical location of the host server
Location where held	Enter the physical location where the asset or service is normally used.
Manufacturer / vendor	Enter the make or service provider
Media identifier	Enter a unique identifier for the media
Model	Enter the release or version of the asset or service etc
NHS IG security requirements	Enter the relevant Information Governance toolkit control requirements
No of Licences	Enter the number of user licences obtained for the software or service.
Owner / authorised user	This is the person assigned responsibility for the asset or service etc.
Practice users of the service	Enter the users of the service at Practice level
Product version no	Enter the product version number of the software or service.
Protective classification	Enter the level of sensitivity that has been assigned
Removable media type	Enter whatever the media type is e.g. USB pen drives, tapes, DVD or CDS etc
Serial No or identifier	Enter the unique manufacturer's or support organisation's allocated device identifier number
Service name	Enter the name the service is known by
Service provider	Enter the provider or the vendor of the service
Service type	Enter what type of service is being provided e.g. bookings, administration etc
Software type	Enter the type of software or application e.g. MS Word etc
Systems where processed	Enter the name of the system where processing occurs

Appendix 3 – Senior Information Risk Owner (SIRO) job role

Post	Senior Information Risk Owner (SIRO)
Role Summary	
The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Trust and advise the Board on the effectiveness of information Risk management across the Trust.	
Specific responsibilities	
The key roles of the SIRO are: – Understands how strategic business goals of the Trust 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 annual information risk assessment; – Review and agree actions in respect of identified information risk; – Ensure that the Trust'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.	
Key Relations (within the Trust)	
– IAOs – Corporate services – Head of Clinical Governance – Records & Information Governance Manager/Data Protection Officer – ICT – Caldicott guardian – IAAs – Users of the information assets owned	
May also have contact with	
– Other NHS organisations and external business partners	

Appendix 4 - Information Asset Owner (IAO) job role

Post	Information Asset Owner (IAO)
Accountable to	Senior Information Risk Owner (SIRO)

Role Summary

Information Asset Owners for Cheshire & Wirral Partnership NHS Foundation Trust are Heads of Operations and Heads of Departments.

The IAO's role is to:

- Understand and address risk to the information they 'own'
- Provide assurance to the SIRO on the security and use of these assets.

Specific responsibilities

The key roles of the IAO are:

- 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 Trust Information Governance strategy and action plan;
- Undertakes regular (annual) reviews on the information risk associated with the asset;
- Understands and addresses risks to the asset and provides assurance to the SIRO
- Knows who has access and why, and ensures their use is monitored and compliant with policy;
- Receives, logs and controls requests from others 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;

Key Relations (within the Trust)

- SIRO
- Other IAOs
- Corporate services
- Head of Clinical Governance
- Records & Information Governance Manager
- ICT
- Caldicott guardian
- IAAs
- Users of the information assets owned

May also have contact with

- Other NHS organisations and external business partners

Appendix 5 - Information Asset Administration (IAA) job role

Post	Information Asset Administration (IAA)
Accountable to	Information Asset Owner (IAO)

Role Summary

Information Asset Administrators will provide support to their IAO to:

Ensure that policies and procedures are followed:

- Recognise potential or actual security incidents;
- Consult their IAO on incident management;
- Ensure Information Asset Register is accurate and maintained up-to-date.

Specific Responsibilities

- Maintenance of Information Asset Register;
- 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 consult 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 Trust Records Policy).

Key Relations (within the Trust)

- IAO
- Head of Clinical Governance
- Records & Information Governance Manager/Data Protection Officer
- ICT
- Caldicott guardian
- Other IAA's
- Users of the information assets owned

Appendix 6 IAO's Annual Report to SIRO

REF	REQUIREMENT	TARGET DATE	AUDIT CONCLUSION	DATE COMPLETED
TRAINING				
1	Has all mandatory information governance training been undertaken by the Information Asset Owner?			
2	Has all mandatory information governance training been undertaken by the Information Asset Administrator?			
3	Has all mandatory information governance training been undertaken by all relevant staff involved with the asset?			
4	Are all relevant staff encouraged to identify and undertake additional information governance to support their roles?			
INCIDENT REPORTING				
5	Do all relevant staff understand incident reporting arrangements relating to information governance incidents including losses of data and/or equipment, breaches of confidentiality etc?			
6	Have there been any losses of person identifiable data (PID) associated with the asset during the current financial year?			
7	Have any losses of person identifiable data been reported appropriately?			
ASSET REGISTER				
8	Is the asset included and properly recorded and updated on the Information Asset Register?			
INFORMATION SHARING				
9	Have all flows of person identifiable information to and from the system/information asset been mapped and any associated risks assessed in line with Department of Health guidelines?			
10	Have safe haven procedures been put in place to safeguard and secure all routine flows of person identifiable data?			
11	Is the mapping information up to date and have risks identified been addressed and mitigated against?			
12	Are there signed up to date information sharing agreements with other organisation and third parties? Please provide a list.			
ORGANISATIONAL AND TECHNICAL MEASURES				
13	Are all laptops used in connection with the asset encrypted?			
14	Are all memory sticks used in			

	connection with the asset encrypted?			
15	Is there an up to date list of staff who are authorised to send asset-related encrypted person identifiable outside the organisation?			
16	Is there an up to date list of staff and contractors with access to the asset or involved in handling person identifiable information or confidential information associated with the asset?			
MONITORING AND RISK ASSESSMENT				
17	Has an annual assessment of risk and performance been undertaken?			
18	Has there been at least one information governance assessment of the asset to review and assess security and access controls?			
19	Is the asset included on the list of assets within the scope of confidentiality audits?			
20	When the asset has been changed or updated, has a data protection impact assessment been carried out in line with confidentiality and Data Protection arrangements?			

Information Asset:

Information Asset Owner:

Reporting Period:

Name:

Department/Service:

Signature:

Date:

Appendix 7 Guidance Notes for Data Flow Mapping

Following incidents of data loss in the public sector, the NHS has brought out a new requirement for all Trusts to map their **key data flows**; put action plans in place to increase data security in transit and report the results as part of the information governance annual assessment. CWP must complete the data flow mapping exercise using the national template and data collection tool.

The mapping covers **ROUTINE** flows of SENSITIVE or PERSON-IDENTIFIABLE DATA into, out of and around KEY AREAS of the organisation. Because of our geographic spread, we may need to include information flowing from one Trust location to another. The mapping covers manual and electronic data – if it is person-identifiable it needs to be mapped.

- **ROUTINE** – routine flows are those that take place on a regular basis – irrespective of the frequency.
- **SENSITIVE** – information about a living individual which includes:
  - Racial or ethnic origin
  - Political opinions
  - Religious beliefs
  - Trade union membership
  - Physical or mental health
  - Sexual life
  - Offences or alleged offences
- **PERSON-IDENTIFIABLE DATA** – information about a person (living or dead) which would enable that person's identity to be established. This may be one piece of information – such as name – or a combination of pieces of information. The most common identifiers are:
  - Name
  - Address
  - Postcode (some postcodes relate to a single property and are therefore included)
  - Date of Birth (in conjunction with other information)

  In CWP this is primarily information about staff, service users and carers, visitors, members and governors but may include stakeholders, partners or contractors.
- **KEY AREAS** – areas of an organisation that have a **significant number** of inbound or outbound person-identifiable data items (e.g. HR Department)
- **INFORMATION ASSET OWNER –** Head of Operations/Head of Department
- **INFORMATION ASSET ADMINISTRATOR -** appointed by Information Asset Owner to monitor information flow
- **PLANNED REVIEW DATE:** Annually
- **INFLOW** - information received in the department/service
- **OUTFLOW** - information leaving the department/service
- **BULK** - bulk data is sensitive or person-identifiable data relating to 50 or more individuals
- **INTERNAL TRANSFERS** - any dept/service within CWP – this may be another site within the Trust.
- **EXTERNAL TRANSFERS -** destination for information is not within CWP eg another Trust, local Council, a country outside the UK
- **AUTOMATED SYSTEM TO SYSTEM TRANSFER –** automatic transfer of information between electronic systems

- **REMOVABLE MEDIA** – eg laptops; PDA's (personal data assistants), Smartphones, Blackberry's, Tablet and slate computers, memory sticks, floppy discs, re-writable CDs and DVDs, magnetic tapes, portable hard drives, secure digital cards.

Notes:

1. Patient Case Notes – **health records can be exempted from mapping where they are transferred from health professionals as part of a normal episode of care.** Any **transfer of clinical records** to courts, solicitors, insurance companies etc. or for destruction or bulk transfer **to external locations should be mapped.**
2. Posting paper – data must be tracked or sent securely. Royal Mail provides two mail services; recorded delivery which is not tracked and special delivery, which is. Recorded delivery is not suitable as a means of ensuring safe carriage for extremely sensitive information. Special delivery or courier services are safer and more secure and recommended for bulk transfer of sensitive or person-identifiable data.

Organisations are not expected to use courier services or special delivery for individual data items (such as appointment letters).