Information Asset Register Procedure

Document History

Document Reference:	IG21
Version:	Final Policy
Ratified by:	SLCCG /SWLCCG Senior Leadership Teams
Date ratified	March 2018
Name of originator/author	Information Governance Services
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

South Lincolnshire CCG
South West Lincolnshire CCG

Version control sheet

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author	Version
Revised Version serving SWL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SL and SWL CCG referenced IG21.	14/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre on the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook and the Privacy Impact Assessment Policy.

CONTENTS

1 INTRODUCTION

1.1 This policy applies to NHS Lincolnshire East Clinical Commissioning Group (CCG) subsequently referred to in this document as 'the CCG'.

1.2 Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure they are protected at all times and are available and accurate to support the operation of the organisation. The CCG must ensure that all information assets that hold or process personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data. There should be formal information security risk assessment and management programme and operating systems under the organisation's control must support appropriate access control functionality

1.3 All information assets of the CCG should be identified and the CCG must have a nominated Senior Information Risk Owner (SIRO). The SIRO is required to ensure owners are identified for all Information Assets, Information Asset Owners (IAOs), with responsibility for managing the risks to those assets. Whilst responsibility for implementing and managing Information Asset controls may be delegated to Information Asset Administrators (IAAs) or equivalent, accountability should remain with the nominated owner of the asset.

1.4 NHS Digital has issued guidance to all NHS organisations on the process to be followed in identifying information assets, and allocating local ownership and responsibility for assessing any risk of data loss or information security for these assets. Guidance is available here: https://digital.nhs.uk/search?q=asset+management&s=s

1.5 It is part of the guidance that risk assessments are performed regularly to ensure that the organisation complies with the Information Governance Assurance Programme and regular risk assessments are a requirement in the Information Governance Toolkit (IGT), which is mandated for all NHS organisations.

1.6 Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisations computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process personal confidential data (PCD) of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

2 OBJECTIVES

2.1 All information assets should be accounted for, understood, have a designated owner and be appropriately protected.

This will ensure compliance with:

2.1.1 The Data Protection Act 2018 and the General Data Protection Regulations (GDPR) when they become law on 25th May 2018

2.1.2 The Caldicott Report and subsequent review on personal confidential data

2.1.3 The Information Security standard ISO 27001/2

2.2 NHS Digital has issued a standard template which can be used for capturing a list of assets, their owners and risk assessments. This is found at **Appendix 1** and is available in Excel format.

3 SCOPE

3.1 The Information Asset Register Procedure applies to all business functions across the CCG, and covers information, information systems, networks, physical environment and relevant people who support those functions. It relates to both manual and electronic information, whether transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed as hard copy (see **Appendix 2** for examples of information assets).

4 INFORMATION ASSET OWNERS (IAOs)

4.1 Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate identified risk (see risk assessment process at **appendix 3**).

4.2 The role of the Information Asset Owner is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The Information Asset Owner will also be responsible for providing or informing regular written reports to the SIRO, a minimum of annually on the assurance and usage of their asset (see **appendix 4**).

4.3 The information asset owner will:

4.3.1 ensure access to the asset is appropriately controlled in accordance with its classification and the CCG's policies on information security, confidentiality, access and information sharing.

4.3.2 ensure that the backup and business continuity arrangements are appropriate in accordance with its classification

4.3.3 ensure that the asset is managed in accordance with the Data Protection Act data protection principles and Caldicott Principles if the information asset processes personal confidential data.

5 INFORMATION ASSETS

5.1 Information Assets (IA) are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. Information assets are likely to include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data. Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

5.2 Business processes and activities, applications and data should all be considered as Information Assets; however, their importance to the CCG may vary (appendix 2).

6 INFORMATION ASSET REGISTER

6.1 Information Assets should be documented in a CCG asset register (IG Toolkit requirement, template at Appendix 1). In practice, a number of CCG asset registers may exist (e.g. departmental, HR Register, hardware register), and many will be *ad hoc*. As a priority, it is essential that all critical Information Assets are identified and included in this asset register, together with details of the 'Information Asset Owner' and risk reviews undertaken. The corporate Business Continuity Plan will also list these as critical information assets.

6.2 Each Information Asset Owner should be aware of what information is held and the nature and justification of information flows to and from the assets they are responsible for.

7 IDENTIFICATION OF NEW ASSETS

7.1 The Information Governance Toolkit has a requirement for a documented plan to be developed to investigate and identify all remaining information assets that comprise or hold personal data and to assign responsibility for any identified, including details in the information asset register.

7.2 The Plan will be implemented by:

7.2.1 Ensuring that Privacy Impact Assessments (PIAs) are included in any procurement process where new systems are implemented. This has a data mapping form within the template to ensure new assets are captured.

7.2.2 The asset register will be reviewed by the CCG on a regular basis (at least annually) and circulated to all staff for them to review and refresh the asset register.

7.2.3 The Asset Register will be reviewed at the Information Governance Committee or equivalent.

8 RISK

8.1 Appropriate security measures must be viewed as necessary for protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address the threat of something damaging the confidentiality, integrity or availability of information held on systems or manual records, the impact that such a threat would have if it occurred, the chance of such a threat occurring.

8.2 All new projects and procurements of IT systems will have a risk assessment as part of the project, and any existing systems should have periodic risk assessments, including those carried out by local management and internal/external audit services. Any risks identified as high must be reported to the Information Governance, Management and Technology Committee (or equivalent) and if appropriate recorded on the IG risk register and/or escalated to the CCG's corporate risk registers and Governing Bodies.

8.3 Controls can then be implemented to reduce the assessed risks in one of the following ways:

8.3.1 Avoid the Risk
8.3.2 Transfer the Risk
8.3.3 Reduce the Threats
8.3.4 Reduce the Vulnerabilities
8.3.5 Reduce the Possible Impact
8.3.6 Detect Unwanted events, react and recover from them

8.4 There will always be residual risks and these should be reviewed on a regular basis to ensure that additional controls are having an effect on the likelihood rating. Risk Assessment Process is **Appendix 3.**

9 EQUALITY IMPACT ASSESSMENT

9.1 The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

9.2 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

10 DUE REGARD

10.1 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

11 PROCEDURE REVIEW

11.1 This procedure will be reviewed in line with Information Governance Toolkit requirements or where changes occur in national policy or legislation.

11.2 **Advice and Guidance -** Please contact the Information Governance Lead or The Commissioning Support Service for further advice relating to the CCG's information asset register.

For advice and assistance in relation to the application of this policy and to obtain updates please contact: your line manager in the first instance or Optum Commissioning Support Unit, Council Offices, St Peters Hill, Grantham, NG31 6PZ e-mail lynne.wray1@nhs.net or jemptage@nhs.net

Appendix 1

EXAMPLE CCG ASSETS

- *The assets **shal**l be categorised using the below list as the framework:*
  - ***Hardware***
    - *Desktops*
    - *Monitors*
    - *Laptops*
    - *Printers*
    - *Media – CDs, DVDs, optical Disks, External Hard Drives, USB memory Sticks (also known as pen drives and flash drives), Media Card Readers, Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards), MP3 Players, Digital Cameras, Backup Cassettes, Audio Tapes (including Dictaphones and Answering Machines), etc.*
    - *Photocopiers*
    - *Fax Machines*
    - *Servers*
    - *Firewalls*
    - *Routers*
    - *Switches*
    - *Tokens*
    - *Keys*
  - ***Software***
    - *Databases*
    - *Applications*
    - *Software Licenses*
    - *Support/Warranty Contracts*
    - *Development software*
    - *Utilities software*
    - *Data files*
  - ***Physical***
    - *Hardcopy documents – files, letters, patient records, etc.*
    - *X-rays, CT Scans, MRI reports, etc.*
    - *Microfiche*

Appendix 2

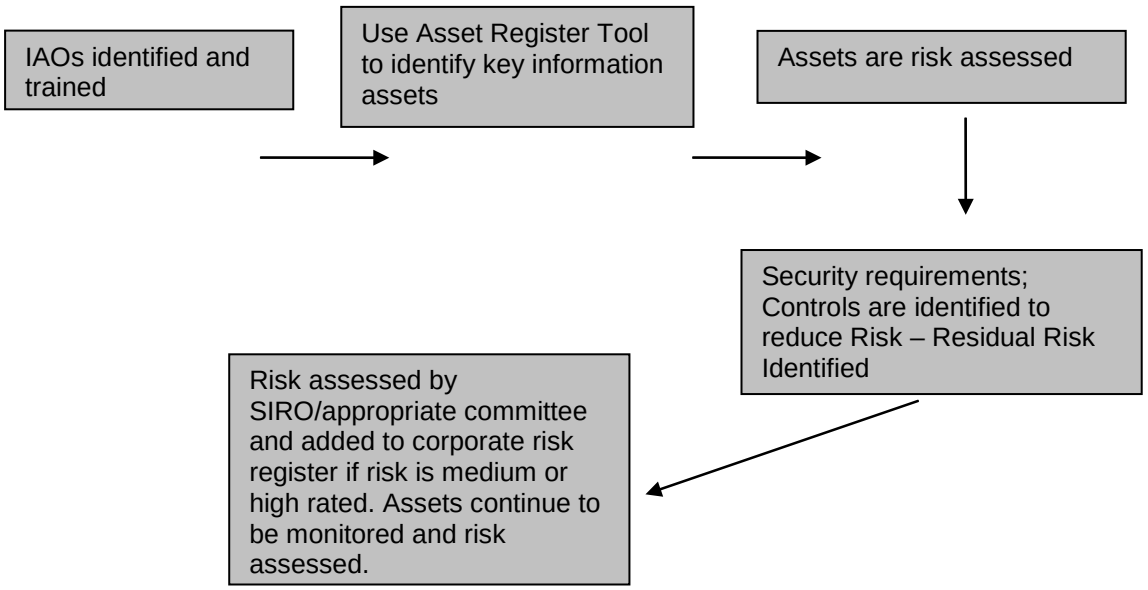
INFORMATION ASSET RISK ASSESSMENT PROCESS

Process

The information asset is risk assessed using the form below on a regular basis (determined by the type of asset involved and whether there have been any major organisational changes). The risk report is reviewed by the Senior Information Risk Owner and any moderate or high risks assessed for reporting on the CCG corporate risk register.

The risk assessment forms are sent out to the IAOs for refresh and update on a regular basis and also for addition of any newly identified information assets.

Overview of Risk Assessment Process



Any new processes, systems or information assets that are introduced will be identified by the IAO in order to ensure that any impacts to information security, confidentiality or integrity are identified prior to implementation and initiation of any new system. Privacy Impact Assessments screening is performed if appropriate using the Information Governance Risk Assessment forms and these are reviewed and approved by the appropriate committee or senior manager.

Appendix 3

INFORMATION ASSET RISK REPORTING TEMPLATE

Date	
Asset Reference	
Information Asset Name	
Information Asset Owner	

Initial Risk Rating			
	Impact	Likelihood	Total
Confidentiality			
Integrity			
Availability			

Actions taken to eliminate/mitigate risk

Current Risk Rating			
	Impact	Likelihood	Total
Confidentiality			
Integrity			
Availability			

Further actions required to eliminate/mitigate risk

Appendix 3 continued **Further risk assessment questions**

Reference	Action	Target/ Deadline	Risk Assessment and Comments	Date Completed
1	Are procedures in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human			
2	Have all flows of PCD been mapped, assessed risks in line with NHS Digital guidelines and put in place safe haven procedures for all routine flows of PCD in the			
3	Does access to the system(s) have documented user access procedures and controls (is access granted only to authorised individuals and is this access reviewed regularly?)			
4	Are there standard operating procedures for the system and/or system level security policies?			
5	Do all staff understand incident reporting arrangements relating to information governance incidents / loss of equipment or data?			
6	Is a backup log maintained and assignment of responsibility for system upgrades and applications?			
7	Have all new users to the system had adequate training? (In system use and confidentiality)			

Appendix 4

RISK ASSESSMENT MATRIX

Risk Priority

Key: Red – High Risk Amber – Medium Risk Green – Low Risk

RISK MATRIX					
5 - Very High	A	A/R	R	R	R
4 - High	A	A	A/R	R	R
3 - Medium	A/G	A	A	A/R	A/R
2 - Low	G	A/G	A/G	A	A
1 - Very low	G	G	G	G	G
Impact	**1 - Rare**	**2 - Unlikely**	**3 - Possible**	**4 - Likely**	**5 - Almost Certain**
	Likelihood				

Risk Matrix – Likelihood

Likelihood rating	Description
Almost Certain	this type of event will happen frequently
Likely	this type of event will happen, but its not a persistent concern
Possible	this type of event may well happen (e.g. 50/50 chance)
Unlikely	unlikely that this type of event will happen
Rare	cannot believe that an event of this type will occur in the foreseeable future

	1	2	3	4	5
DESCRIPTOR	**INSIGNIFICANT**	**MINOR**	**MODERATE**	**MAJOR**	**CATASTROPHIC**
Injury	Minor injury not requiring first aid	Minor injury or illness, first aid treatment needed	Over three days off "sick" = **RIDDOR** reportable. 10 days to report to the HSE.	Major injuries, or long term incapacity / disability (loss of limb)	Death or major permanent incapacity
Patient Experience	Unsatisfactory patient experience not directly related to patient care	Unsatisfactory patient experience - readily resolvable	Mismanagement of patient care – short term effects	Mismanagement of patient care – long term effects	Totally unsatisfactory patient outcome or experience
Complaint/ Claim Potential	Locally resolved complaint	Justified complaint peripheral to clinical care	Justified complaint involving lack of appropriate care	Multiple justified complaints	Multiple claims or single major claim
Objectives/ Projects	Insignificant cost increase/schedule slippage. Barely noticeable reduction in scope or quality	< 5% over budget/schedule slippage. Minor reduction in quality/scope	5 -10% over budget/schedule slippage. Reduction in scope or quality requiring client approval	10 - 25% over budget/schedule slippage. Doesn't meet secondary objectives	> 25% over budget/schedule slippage. Doesn't meet primary objectives
Service/ Business Interruption	Loss/interruption > 1 hour	Loss/interruption > 8 hours	Loss/interruption > 1 day	Loss/interruption > 1 week	Permanent loss of service or facility
Human Resources/ Organisational Development	Short term low staffing level temporarily reduces service quality (< 1 day)	Ongoing low staffing level reduces service quality	Late delivery of key objective/service due to lack of staff (recruitment, retention or sickness). Minor error due to insufficient training. Ongoing unsafe staffing level	Uncertain delivery of key objective/ service due to lack of staff. Serious error due to insufficient training	Non-delivery of key objective/ service due to lack of staff. Loss of key staff. Very high turnover. Critical error due to insufficient training
Financial	Small loss (> £100)	Loss > £1,000	Loss > £10,000	Loss > £100,000	Loss > £1,000,000

	1	2	3	4	5
DESCRIPTOR	**INSIGNIFICANT**	**MINOR**	**MODERATE**	**MAJOR**	**CATASTROPHIC**
Inspection/ Audit	Minor recommendations. Minor non-compliance with standards	Recommendations given. Non-compliance with standards	Reduced rating. Challenging recommendations. Non-compliance with core standards	Enforcement Action. Low rating. Critical report. Multiple challenging recommendations. Major non-compliance with core standards	Prosecution. Zero Rating. Severely critical report
Adverse Publicity/ Reputation	Rumours	Local Media - short term	Local Media - long term	National Media < 3 Days	National Media > 3 Days. MP Concern (Questions in House)

Risk Matrix – Descriptor of Impact

Appendix 5 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Information Asset Register Policy

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

Name(s) and role(s) of staff completing this assessment:

June Emptage – Information Governance Officer

Date of assessment: 15 February 2018

Please answer the following questions in relation to the proposed change:

Will it affect employees, customers, and/or the public? Please state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.