Information Asset Acceptance and Registration Procedure

Version:	2.2
Bodies consulted:	-
Approved by:	Governance Manager
Date Approved:	7.9.16
Lead Manager	Governance Manager
Lead Director:	SIRO
Date issued:	Mar 17
Review date:	Feb 19

Is this policy current? Check the intranet to find the latest version!

Contents

Information Asset Acceptance and Registration Procedure

1 Introduction

The Trust recognises the importance of protecting and managing personal data by knowing and managing the information assets in which data are stored. The principle way of exercising effective control is to ensure that any prospective addition to the register is properly considered so that any risk can be mitigated, and that a record is kept of all controls that are in place.

2 Purpose

This procedure sets out the Trust's definition of what an information asset is and how they might be accepted then recorded on the register.

3 Scope

For the purposes of registration, only assets containing personal identifiable information will be included, and only where the Trust is the Data Controller, Joint Data Controller, or Data Controller in common. Outputs from assets, eg reports, would not necessarily constitute new assets.

Where assets have already been accepted by the Trust through the Due Diligence for New Prospects Procedure, the asset owner can skip sections 6a and 6b.

Use of assets without registration would constitute an incident and must be reported using the incident procedure.

4 Definitions

Information Assets
Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, records and information.

Personal confidential information

Information about a person which would enable that person's identity to be established. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Privacy Impact Assessment
A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions.

5 Duties and responsibilities

Chief Executive
The Chief Executive is responsible for the protection of all personal data; in practice, the management of individual assets is delegated to Information Asset Owners.

Senior Information Risk Owner (SIRO)
The SIRO is responsible for overseeing the management of all assets and ensuring owners comply with mandatory requirements. The SIRO shall report his findings to the Clinical Quality, Safety, and Governance Committee.

Governance Manager
The manager will write and update this procedure to ensure that new or proposed changes to organisational processes or information assets are identified; maintain an asset register; and report to the SIRO on the status of individual IAO's compliance. The manager will be responsible for deciding whether a proposal is suitable for consideration by the IM&T Strategy Group.

Caldicott Guardian
The Caldicott Guardian is available for advice and guidance on all patient related confidentiality matters.

Information Asset Owner
Information Asset Owners (IAOs) are directly accountable to the Chief Executive and must provide assurance that information risk is being managed effectively and that related procedures followed in respect of the information assets that they 'own'. Information Asset Owners will be responsible for the supervision of respective Information Asset Administrators.

Information Asset Administrator

Information Asset Administrators (IAA) are usually operational members of staff who understand and are familiar with information risks in their area or department, eg. directorate managers and administrators. Information Asset Administrators will implement the organisation's information risk policy and risk procedures for those information assets they support and will provide evidence of compliance to the relevant Information Asset Owner as necessary.

Data Owners
Data owners will be responsible for:

- specifying how the data can be used;
- agreeing who can access the data and what type of access each user is allowed;
- ensuring compliance with security controls;
- ensuring compliance with information governance procedures

All staff
All staff must follow this procedure.

Health and Safety Manager
The Health and Safety Manager is available to advice on all aspects of risk management.

Information Communication and Technology Manager
Will ensure that proposals are compatible with existing ICT systems and that technical capacity to introduce and manage the assets thereafter is available.

Directors
Directors are responsible for ensuring that their staff comply with this procedure for all assets in their directorate. Directors will confirm that they are content with a proposal being proposed

6 Procedures

Proposer	A range of agreements must be secured before IG approval can be considered
Prospective registration	A form logging consultation with the Trust's subject matter experts is completed
Director agrees proposal can go forwards	A director should consider how the investment fits with the directorate's aims and the Trust's strategic plan
Detailed assessments	These may include specific assessments for health applications, ICT compatibility checks
IM&T Steering Group considers proposal	The Group will consider the proposal in the context of various priorities and demands and schedule implementation accordingly
Full registration as an asset	IM&T approval does not give general approval -there may be other contractual or financial approvals that must be secured from others, or high level approval for major proposals
Maintaining registration	The onus is on the IAO to ensure that the asset is safe and fit for purpose

a) Prospective registration

Those responsible for managing systems containing data will be regarded as the "data owners" of that data. For example, for the *CareNotes* and SBS systems Managers are the data owners of data on those systems. The Governance Manager, Caldicott Guardian, Information Security Lead, and the ICT Manager can provide advice on security and compliance, with relevant legislation.

Any data owner who either identifies, or who is advised by any of the people listed in section 4, prospective asset owners should follow the process outlined in appendix C.

The Executive Management Team members will be invited to annually review the current list of assets for accuracy, completeness, and obsolescence.

If the Governance Manager determines that a set of data is an information asset, then the Governance Manager will confirm that the owner of that data set is the IAO (or identify an owner if necessary).

b) Feasibility of acquisition

It is for the prospective IA owner to ensure that acquisition of an asset is managed with proper controls and safeguards in place; this is achieved in part by ensuring that the senior managers with subject matter expertise and been engaged to consider all issues and risks. This applies to both the process of acquisition and the management of the asset thereafter. The form at appendix 3 must be completed and sent to the Governance Manager. Where positive answers cannot be given at the time the form is completed, a plan must set out how that section is to be completed.

The Trust does not have the resources nor expertise to be able to assess any and every proposed application; no applications relating to personal health other than those already approved by competent NHS bodies at national level will be considered.

Only when feasibility has been established can an asset be registered and used.

c)   Asset registration
Once the asset has been accepted, the IAO has one month to ensure the following are completed:

- nomination of IAA
- undertake training as directed by the Governance Manager, and ensure IAA undertakes training
- complete a log of essential information
- completes risks assessments as directed by the Governance Manager
- completes a Privacy Impact Assessment if required
- completes a data map

The Governance Manager will

- inform the Caldicott Guardian if the asset contains patient data
- inform the Deputy Chief Executive if the asset is a corporate or DET record
- provide expert support as required

d) Maintaining registration

Information assets will be managed by suitably trained IAOs to oversee their day to day running and to preserve information security and integrity in collaboration with the owners of those assets.

e) Changes to registration

Changes to Information Assets will be carefully planned and managed; all changes to assets will be properly tested and authorised before moving to the live environment.

Vendor supplied modifications to Information Assets will only be permitted under strictly controlled circumstances and with the authorisation of the owner of the relevant assets.

f) Monitoring registration

The Executive Management Team members will be invited to annually review the current list of assets for accuracy, completeness, and obsolescence.

The Information Governance work stream of the CQSG will monitor compliance against the requirements set by NHS Digital.

7   Training Requirements

All staff will receive awareness training via the Trust INSET days and corporate/clinical induction, and targeted training will be used where specific issues are identified.

Tailored training is given annually to each member of staff through the IG training toolkit. Specialist training shall be provided for those people in specialist roles as part of their PDP.

8   Process for monitoring compliance with this Procedure

The status of compliance as listed in section 6 (b) and 6 (c) will be recorded on the Information asset Register and reported to the Governance Manager.

Where areas of actual and/or perceived risk are identified, mitigation will be monitored through the Trust's risk/incident management procedures.

9   References

Data Protection Act (1998)

10 Associated documents[1]

Related policies and procedures (available via trust intranet site)

- Information Governance Policy
- Corporate Records Procedure
- Data Protection Policy
- Freedom of Information Procedure
- Incident Reporting Procedure
- Privacy Impact Assessment Procedure
- Risk Management Procedure
- Business Continuity Plan
- ICT Procedure
- Procedure for electronic communication
- Security of premises and assets procedure

---

[1] For the current version of Trust procedures, please refer to the intranet.

Appendix A : Equality Impact Assessment

Completed by	Jonathan McKee
Position	Governance Manager
Date	7.9.16

The following questions determine whether analysis is needed	Yes	No
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		x

Appendix C : prospective information asset assessment

Name of prospective asset	
Service(s) / department(s) in which the asset would be used	
Data that would be held	
Purpose for which data would be held	
Those who would have access to this data	
Immediate and long-term costs identified and funding availability confirmed by finance?	
Finance has confirmed prospective procurement conforms to SFIs?	
ICT compatibility confirmed by ICT manager?	
Are there any communication or marketing issues (if so, please confirm that the Communication Manager has been consulted)	
Are there any issues relating to employment or training (if so, please confirm that the HR Manager has been consulted)	
If any patient user data would be held has the Caldicott Guardian confirmed that the application is compatible with the Confidentiality Code of Conduct?	
Has the Data Governance Manager confirmed that the application would be compatible with EU law?	
Has the Governance Manager approved the contract/ agreement to use?	
Name of director who confirms that they have accepted responsibility for this asset based on the above approvals?	

Name of manager completing this form	
Date	

Please send to governance manager when complete; a response will be provided within 5 working days of receipt.

Office use only

Form received	
Queries raised	
Decision	
Added to IAR	
Registration process booked	
First report due	

Appendix 2: Information Asset Acceptance and Registration Process

```
                          ┌─────────────────────────┐
                          │       Start here        │        ┌──────────────────┐
                          │ Is the entity a service,│        │ The entity is not│
                          │ application, record, or │───────▶│ an information   │
                          │ other entity processing │        │ asset            │
                          │ personal confidential   │        └──────────────────┘
                          │ data?                   │
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐
                          │ Secure subject matter   │
                          │ expert approval         │
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐        ┌──────────────────┐
                          │ Has a prospective       │        │ The process      │
                          │ information asset       │───────▶│ cannot continue  │
                          │ assessment been accepted│        │ until approval is│
                          │ by the Governance       │        │ obtained         │
                          │ Manager?                │        └──────────────────┘
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐
                          │ Is it a personal health │
                          │ application?            │
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐
                          │ Has the application been│
                          │ approved by an competent│
                          │ NHS authority?          │
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐
                          │ Has the application been│
                          │ assessed using the      │
                          │ THAAT?                  │
                          └─────────────────────────┘
                                     │
                          ┌─────────────────────────┐
                          │ IM&T Steering Group to  │        ◆ Approved ◆
                          │ consider approval (and  │───────▶
                          │ schedule introduction)  │
                          └─────────────────────────┘
```

- GM to open new comprehensive inventory
- IAO to nominate IAA
- IAO and IAA to undertake training → certificates
- IAA to complete registration → log
- Complete IG risk assessments → Completed risk assessments
- If high risk then...
- ...GM to inform SIRO
- GM to determine whether PIA is required → Completed PIA
- IAO to complete data map → Data map

- Comprehensive inventory
- IG work stream reporting
- SIRO