East London NHS Foundation Trust

Information Asset Privacy by Design Procedure

Version:	1
Ratified by:	Quality Committee
Date ratified:	27.8.18
Lead Manager:	IG Manager
Lead Director:	Director of Planning and Performance
Circulated to:	all staff via intranet
Date issued:	July 2018
Review date:	Jun 2020
Target audience:	Staff managing data processes

Version Control Summary

Version	Date	Author	Status	Comment
1	5.7.18	J. McKee	Final	approved by IG Steering Group

Contents

Information Asset Privacy by Design 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. Good management and good governance includes a range of considerations, tasks, and processes, of which information governance (IG) is only a part. 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. The Data Protection Act (2018) requires that all plans relating to personal data are referred to the Data Protection Officer so that the people's rights are protected, this is known as *privacy by design.* At this Trust, any proposal involving personally identifiable data must follow this process.

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. A balance needs to be struck between innovation, risk, and resources. The Trust does not have the resources to develop every idea and proposal and this process allows decisions to be made on the basis of fit with the Trust's strategy and in the context of good risk management. Some projects may not fit with strategy and may be high risk, this process does not prevent such proposals, but it will require proposers to set out how they will manage the associated risks so that the Trust can proceed on the basis of understanding.

For the purposes of this process, 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. However, this process may be appropriate even where anonymised data is used where there is any risk that that data could be de-anonymised.

The process is designed to be tailored to three asset types: services; clinical information systems; and non-clinical information systems.

There is no need to use this procedure when expanding an existing activity, unless the expansion itself constitutes a significant risk to an individual's rights.

No 'approval' from at any stage constitutes permission to proceed, only the process as a whole when completed constitutes approval; eg, IG 'approval' does not bind finance to approve, nor *vice versa*. Any approval by a body or an opinion from a subject matter expert is necessarily contingent on having all other proper controls in place and completing registration.

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

3 Definitions

Information Assets

Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, records, and data sets (eg service, audit, research, quality improvement).

Personally identifiable 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.

Data subject

This is the person/persons whose personal confidential information has been collected.

Data Protection Impact Assessment

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

Types of assets

Assets can be electronic or paper based, broadly there are three types:

Systems

These include archive stores, IT infrastructure, electronic information systems; eg RiO, EMIS, NHS Jobs.

Data sets

These are distinct sets of data managed in a unique way designated by an information asset owner, probably across many locations, possibly across several services. Prospective asset owners are advised that as each data set information asset needs to be managed locally, only where substantial differences of management are needed for service reasons should a data set be separated from a larger asset; it is unlikely that micro-management will aid good governance.

Services

Whilst a service is unlikely to be an information asset in itself, the acquisition or divestment of a service will involve substantial project management of information assets that the director for that service is responsible. Therefore, part of the planning and project management must include data protection.

4 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 risk management of all assets and ensuring owners comply with mandatory requirements.

Subject matter expert

The Trust employs a range of SMEs to support staff to make safe decisions about proposals and day to day business. Where indicated, and SME must be consulted. Although a negative opinion from and SME must be addressed, this does not necessarily mean that something cannot go-ahead; however, the proposer will have to document a response and put any mitigating actions into effect. SMEs are listed on the associated form; additional information is included below where relevant.

Data Protection Officer

The Data Protection Officer (DPO) will not approve proposals, but must be consulted at the planning stage and throughout the entity's life-cycle where change occurs. This is a legal requirement.

The DPO selects and introduces a suitable Data Protection Impact Assessment to ensure that new or proposed changes to organisational processes or information assets are identified; maintains an asset register; ensures arrangements are transparent; and reports to the Information Governance Committee on the status of individual IAOs' compliance.

Information Asset Owner

Information Asset Owners (IAOs) are 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' according to guidance issued by the regulator. Information Asset Owners will be responsible for the supervision of respective Information Asset Administrators.

IAOs are 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 related Trust procedures;
- spot checking compliance;
- and reporting as required.

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.

Clinical Systems Programme Manager

Will ensure that proposals are compatible with existing clinical systems and that technical capacity to introduce and manage the assets thereafter is available. Where new proposals are presented, the manager will assess the priority in the context of existing projects and programmes and present findings to the Information Programme Board for decision.

Clinical Systems Manager

The manager is the asset owner for all clinical systems and will lead on the maintenance of clinical systems.

Proposer/ project manager

Unless designated otherwise, the manager leading on taking a proposal through this process will be deemed to be the project manager. Please note that no subject matter expert can be designated as a project manager unless they are also the proposer without clearing the request first. The proposers task is to manage the proposal according to this procedure.

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, and consider the report from the project manager recommending that a proposal be put forwards for detailed assessment. Directors must ensure that assets under their control are subject to reviews and audit.

a) Acceptance and registration process overview

Stages of the IG assessment overview

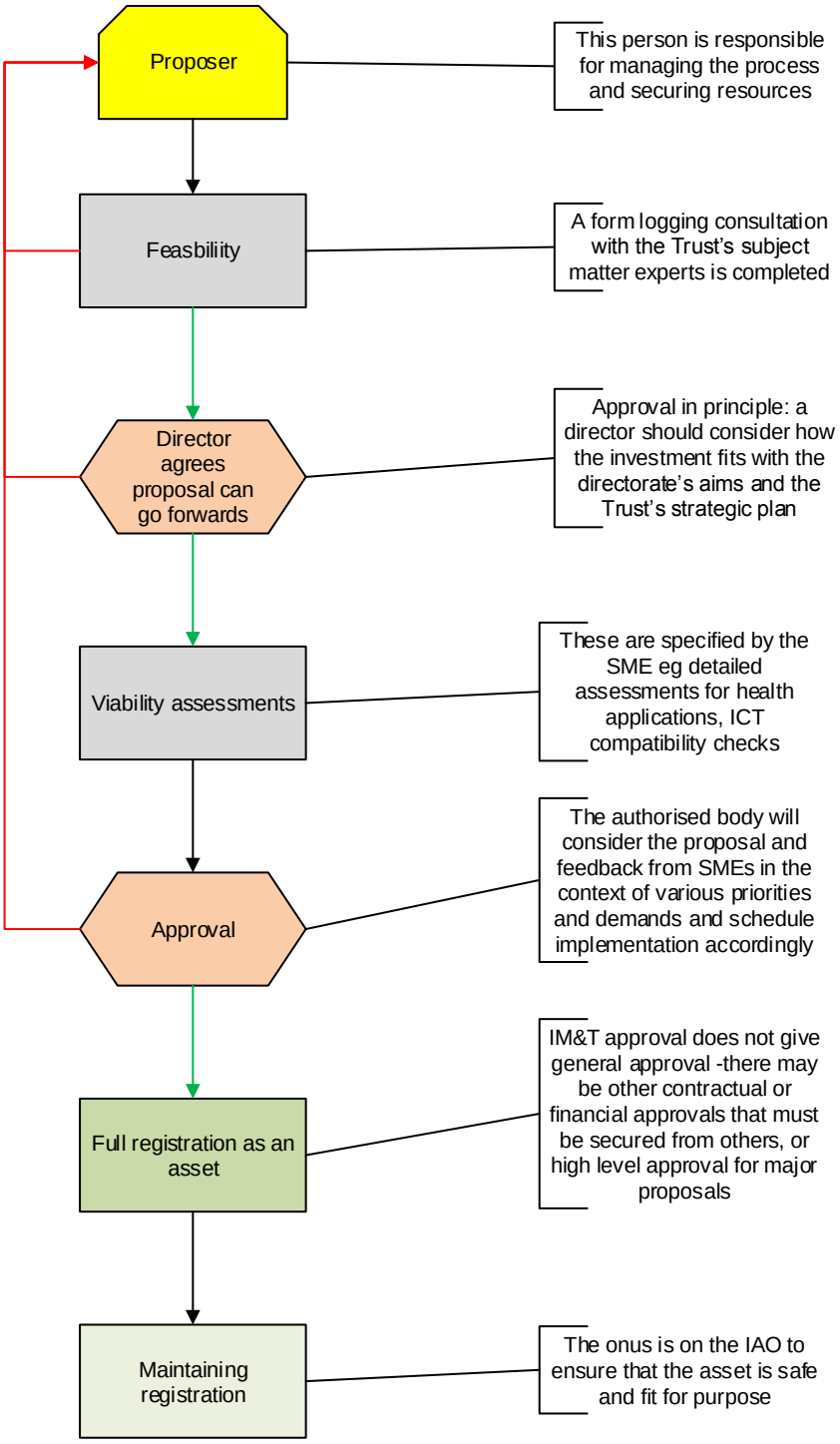


Fig 1: process overview

b) Developing a proposal

In deciding whether to proceed with a proposal, it is for the proposer to make the case for the prospective asset, including the case for others investing time in developing the

proposal. All elements of security and durability are inter-connected, for example, funds to pay for it, implications for training, and data security.

The first task is to set out what the entity is, what the features of it are, how it will benefit the Trust (that is, help deliver the strategy), and how this puts users at an advantage. At this stage, the proposer needs to engage subject matter experts in order to understand what controls would need to be put in place in order to manage the prospective asset safely once it is in place, should the proposal be approved. At this stage, and hereafter, the proposer needs to complete the Trust's form and presents the completed version at various stages for approval. The master copy will be kept on a shared drive allocated by the DPO.

c) Feasibility of acquisition

The purpose of this stage is to identify which proposals will go forwards for development, and which will not. A proposer who is advised by any of the people listed in the feasibility section of the proposal form, must undertake an assessment with the respective subject matter expert to ascertain whether the proposal is feasible. A subject matter expert (SME) will not prevent a proposal going forwards, but any director approving a proposal deemed unsuitable by a SME is unlikely to secure final approval at a later stage.

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 proposer needs to map out the remaining process and identify the approval body. The approval body will depend on the size, cost, and asset type; for example, major projects may need Board approval whilst others could be approved at directorate level -SMEs will be able to advise.

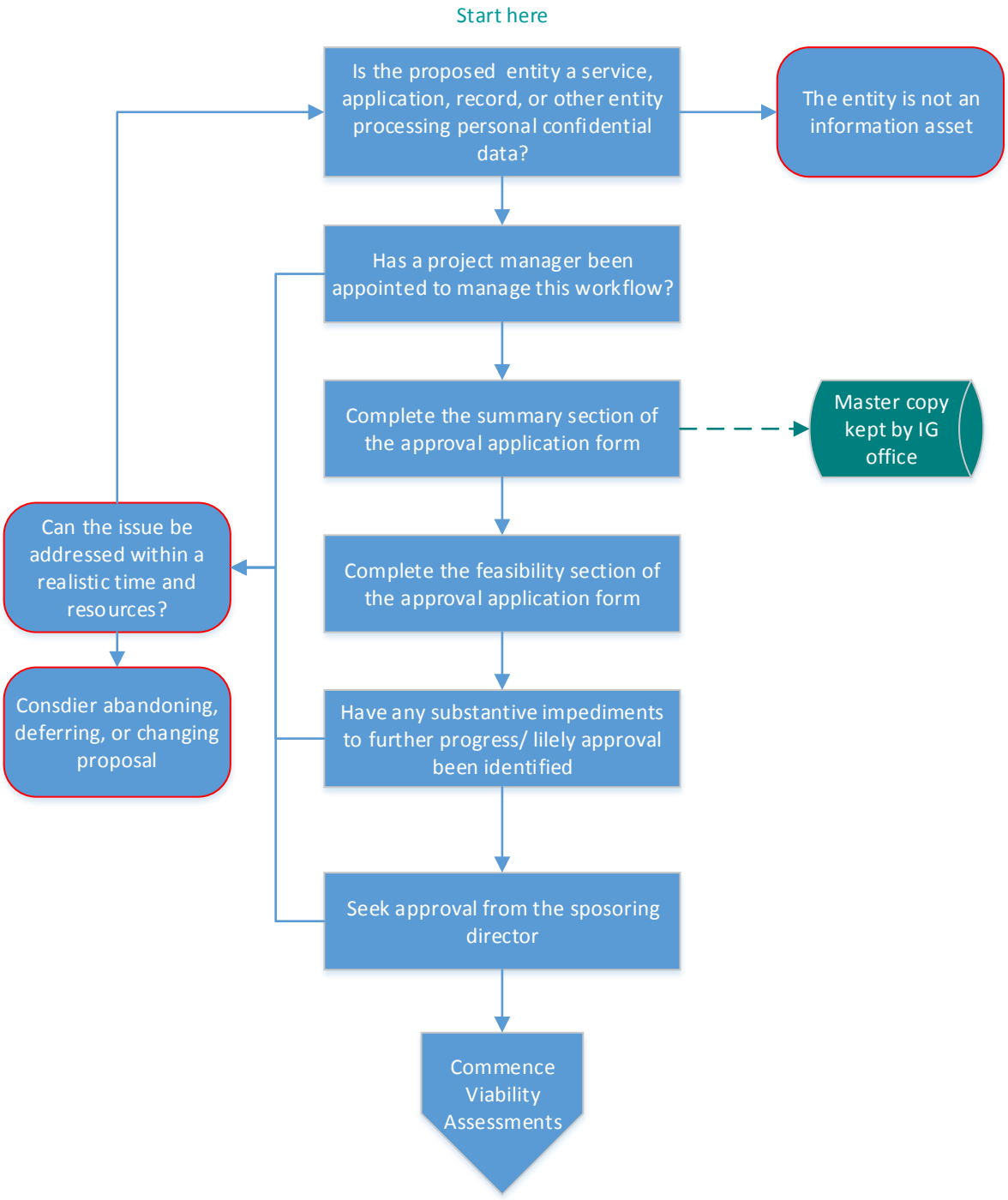


fig 2: feasibility process

Any proposal must be clear about consulting users, whether patients, or staff (for HR systems). Existing consultation processes should be used wherever they exist.

The proposer will also need to set out how the proposal will be project managed to completion; project management is the responsibility of the proposer.

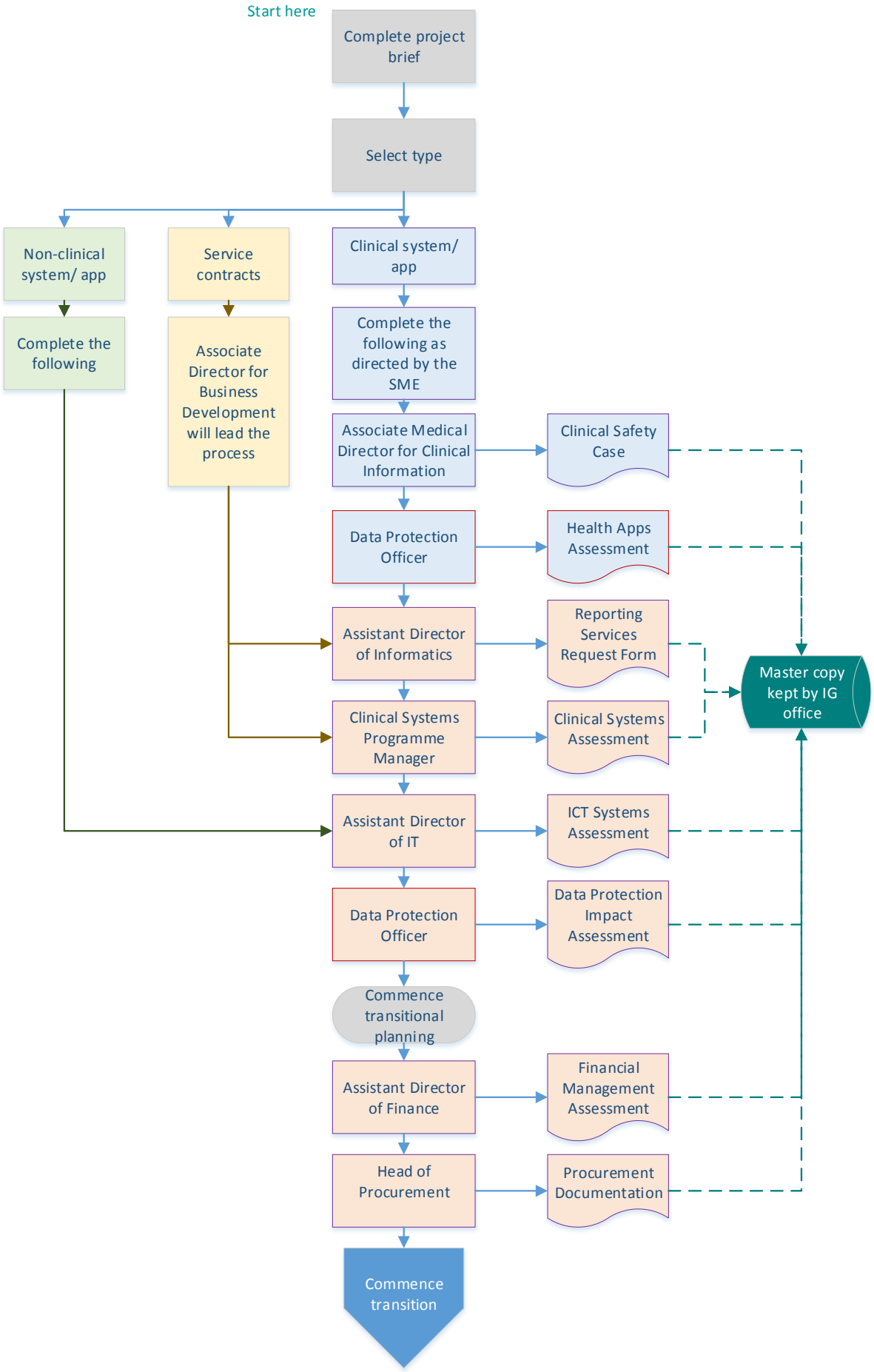
When the sponsoring director is satisfied that there is sufficient understanding of the issues and risks, they may grant approval to proceed to an assessment of viability.

c) Viability assessment

A proposer who is advised by any of the people listed in the feasibility section of the proposal form, must undertake assessments with the respective subject matter expert to ascertain whether the proposal is viable in the foreseeable future. Not every proposal will require every assessment, sometimes they will not apply and sometimes information supplied at the feasibility stage will be enough.

The level of project complexity will be tailored to the entity, but the same project approach will apply to all proposals. It is for the proposer/ project manager to secure approval from the appropriate entity based on their plan and the reports from the SMEs.

The same basic process applies in all cases, though the extent of assessment is tailored to the scale of the entity, and/ or risk as assessed by an SME. Additional detail for 'health apps' and prospective service acquisitions is set out in appendices A and B. The viability process is set out below.


Start here
Complete project brief
Select type
Non-clinical system/ app
Service contracts
Clinical system/ app
Complete the following
Associate Director for Business Development will lead the process
Complete the following as directed by the SME
Associate Medical Director for Clinical Information
Clinical Safety Case
Data Protection Officer
Health Apps Assessment
Assistant Director of Informatics
Reporting Services Request Form
Master copy kept by IG office
Clinical Systems Programme Manager
Clinical Systems Assessment
Assistant Director of IT
ICT Systems Assessment
Data Protection Officer
Data Protection Impact Assessment
Commence transitional planning
Assistant Director of Finance
Financial Management Assessment
Head of Procurement
Procurement Documentation
Commence transition

d) Project management

If indicated, a project group may be established, at which a project plan will be approved. For some projects this will be very light-touch, for others, complexity will be commensurate with risk and scale.

Towards the completion of an implementation project, the project manager needs make arrangements to transition the project to business-as-usual activity to ensure that the asset is cared for after implementation.

e) Asset registration

Towards the completion of an implementation project, the project manager needs to identify the Information Asset Owner (IAO), who will then:-

- Nominate an IAA
- undertake training as directed by DPO
- ensure IAA undertakes training
- complete a log of essential information
- completes risks assessments as directed by the DPO
- completes a Data Privacy Impact Assessment if required
- completes a data map

The DPO will:-

- arrange for registration of the asset
- advice on management and reporting arrangements
- provide expert support as required

f) Approval

The approval body will depend on the entity being proposed; certain proposals will need formal sign-off, see Standing Financial Instructions and Standing Orders for more details. Prior to final approval, the onus is on the proposer to manage the process and ensure consultation has taken place as indicated.

Proposers must understand that approval is contingent on a wide range of factors, and that approval for a proposal does not mean that a proposal will become a project instantly. Proposers will be required to engage with other colleagues and agree when a project will be scheduled, taking into account existing and planned work overall and scheduling new projects if resources allow. Where there is no, or limited, available capacity to undertake a project, the entire project will be shelved until such time as resources have been found. It is, therefore, always useful to use project management approaches tailored locally, in this way, issues of capacity and process can be captured and managed to best effect.

Proposers should work on transitional arrangements as soon as possible to ensure that the asset can be used once approved.

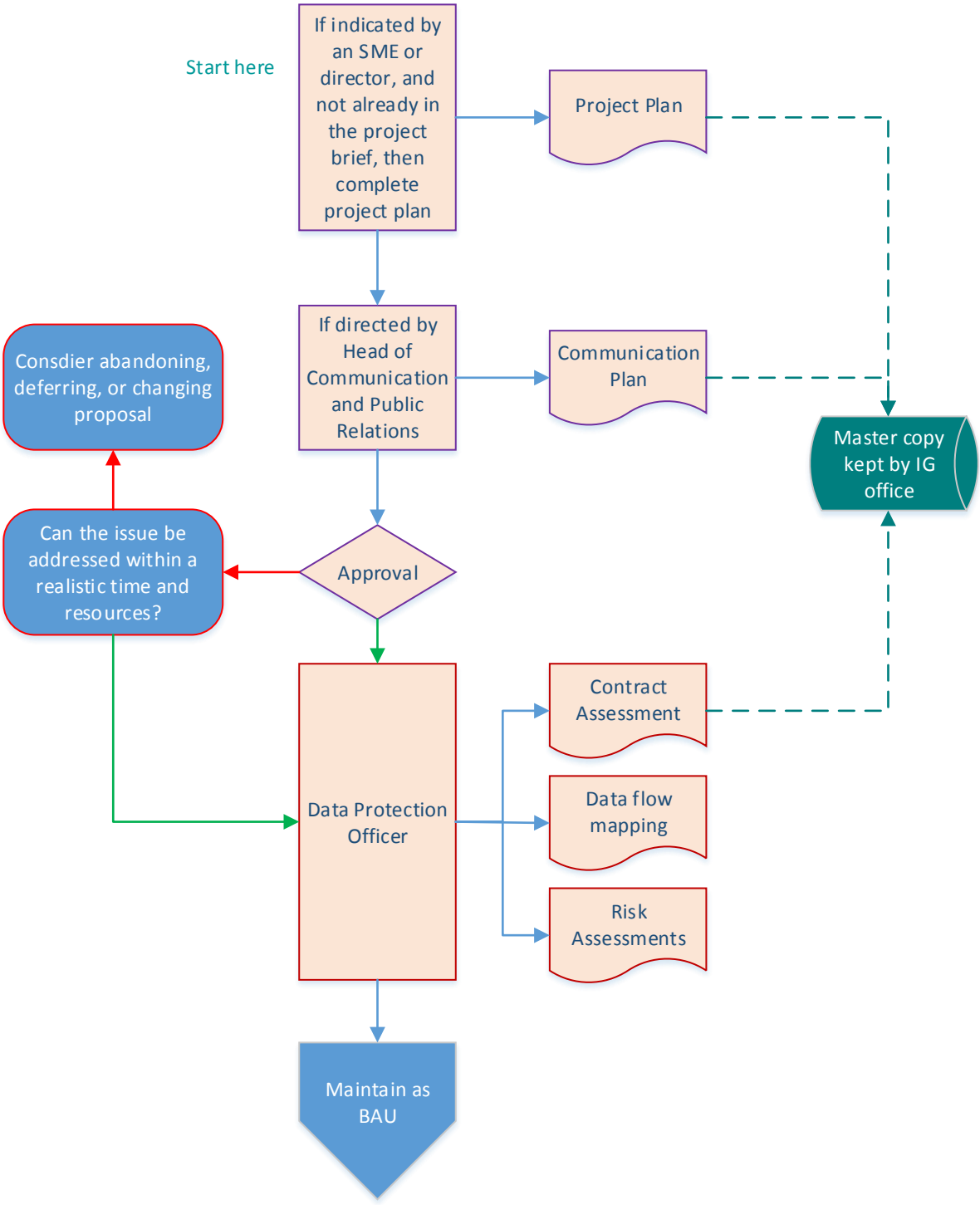


Fig 4: transitional arrangements to registration

f) IA registration

Once a project has been approved, the project manager must make arrangements with the DPO to ensure that the safety of data can be assured. This is done through the IA registration process. The process must be complete before the entity goes 'live'. The process includes:-

- mapping data flows

- undertaking Data Protection Impact Assessments (risk)
- completing a training needs analysis
- learning about spot-checking and monitoring
- reporting of conformance with the above.

g) Maintaining registration

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

Changes to Information Assets will be carefully planned and managed; all changes to assets must be properly tested and authorised before moving to the live environment. Any substantial change must be subject to consultation with data subjects.

Vendor supplied modifications to Information Assets will only be made under controlled circumstances and with the authorisation of the respective subject matter experts of the relevant assets.

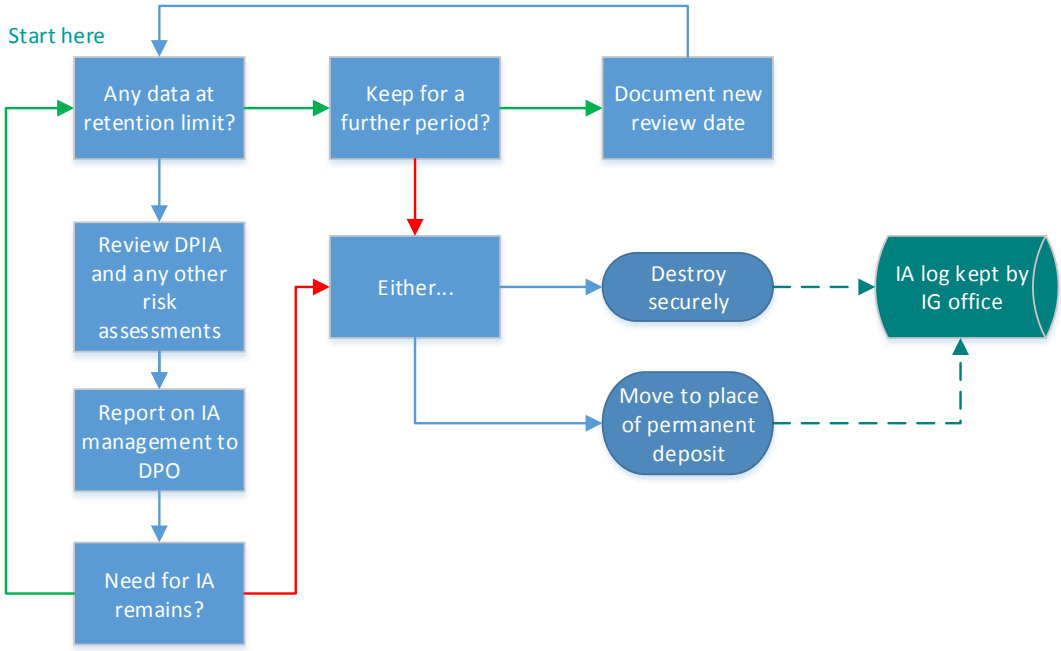


Fig 5: maintaining registration/ decommissioning an asset

Every year, the IAO must ensure that a review of the asset is undertaken to determine:

- that the asset is still needed
- that risk ratings are current
- that risk mitigations are still effective

IAOs must report their findings to the DPO.

h) Decommissioning assets

When as asset is reaching the end of its life, the IAO must make arrangements for it to be put out of use and for the data to be archived.

i) Monitoring registration

The Information Governance Committee will be invited to annually review the current register of assets for accuracy, completeness, and obsolescence.

The Information Governance Committee will monitor compliance against the requirements set by NHS Digital.

5 Training Requirements

All staff will receive awareness training via corporate/clinical induction. IAO and IAAs will complete advanced mandatory training 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.

6 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 Data Protection Officer.

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

7 References

Data Protection Act (2018)

GDPR Working Party Article 29 of Directive 95/46/EC Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

GDPR Working Party Article 29 of Directive 95/46/EC Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)

GDPR Working Party Article 29 of Directive 95/46/EC Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)

8 Associated Documents

Related policies and procedures (available via trust intranet site)

- Information Governance Policy
- Corporate Records Procedure
- Data Protection Procedure

- Freedom of Information Procedure
- Incident Reporting Procedure
- Risk Management Procedure
- Business Continuity Plan
- IT Framework
- Security of premises and assets procedure

Appendix A: 'health apps'/ general guidance

Definition: these are divided into four broad types:-

1. Information provider ~these simply supply existing general or anonymised information, but not personalised advice, to a device, eg BNF online, though they may be targeted at a specific group, eg weight loss tips

2. Personal data provider ~uses data to facilitate care, eg to book appointments online, request repeat prescriptions, recall personal data for health purposes

3. Accessory to a medical device ~apps that collect and send personal data eg measurements, where the output assists the assessment process

4. Medical device ~supports decision making by making calculations or makes decisions having applied algorithms or clinical guidelines.

In addition to these, general apps for communication, including email or video conferencing for clinical interactions, may transmit personal data and be clinically useful, should be considered information assets if they store personal data.

The first category does not involve patient data and does not need IG assessment, though other SMEs make wish to take a view so should be consulted.

The last category requires that the app has been subject to exhaustive assessment and will have a CE mark. It does not *then it cannot be used*; the Trust does not have the resources to asses medical devices.

For data providing apps and medical device accessories, the Trust will use the Tavistock Health App Assessment tool (THAAT).

Appendix B : consideration of service acquisition