The Regulation and Quality Improvement Authority

Information Asset Register Procedure

Produced by the Business Support Unit

Regulation and Quality Improvement Authority

Title:	RQIA Information Asset Register Procedure		
Ownership:	Head of Business Support Unit, RQIA		
Approval By:	Executive Management Team (EMT)	Approval Date:	4 January 2022
Operational Date:	1 March 2022	Next Review:	January 2025
Version No.	2.1	Supersedes:	2.0
Key Words:	Data Protection, Confidentiality, Responsibility		
Director Responsible:	Head of Business Support Unit, RQIA		
Lead Author Position:	Head of Business Support Unit, RQIA		
Additional Author(s):	Data Protection Officer (DPO), BSO		
Department:	Business Support Unit		
Links to other Policies:	Data Protection & Confidentiality Policy		
	Information Security Policy		
	Information Risk Policy		

Table of Contents

1. Introduction

1.1 The Regulation and Quality Improvement Authority (RQIA) understands the importance of identifying, recording and classifying our assets and utilise an Information Asset Register (IAR) to retain a complete list of all current assets, their location, business value, access and risks. RQIA has a legal responsibility to manage its information assets, principally to comply with data protection, contractual and security arrangements.

1.2 Managing information assets is also paramount to the continuity of RQIA's core business, and its corporate reputation.

1.3 The purpose of this document is to help Information Asset Owners (IAOs) to ensure the completion, and maintenance of, RQIA's Information Asset Register (IAR).

1.4 It is important to remember that an IAR is a 'living' register, and should be:

- Reviewed periodically (bi-annually)
- Updated as required. For example, when:
    - New assets are created
    - Old assets are archived
    - Risks or flows associated with an asset changes

2. Definitions

2.1 The National Archives defines an information asset as "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently".

2.2 For the purposes of this document, RQIA defines an ' Information Asset' as any item, system, application or entity that has potential or actual value to the organisation. Such assets include, but are not limited to:

- Information (including personal data);
- Systems;
- Applications (and information stored within them);
- Servers; and
- Datasets (to include databases and spreadsheets, etc.).

2.3 An IAR is a means to help RQIA record all its information assets, and the records, flows, risks and controls associated with them.

2.4 The management of information assets is the process of identifying; classifying, managing, recording and coordinating RQIA's information assets ensure their security and the protection of any confidential data RQIA stores or gives people access to.

2.5 To support the IAR, and assist in determining risk, RQIA also uses two further means of analysing the information assets:

- Information Flow Register (IFR): Designed to capture all information arriving at, or coming from, an information asset; and
- Corporate Records Inventory (CRI): To catalogue all records associated with an information asset and which exist within RQIA, regardless of format / media.

3. The Information Asset Register (IAR)

3.1 Every information asset owned by RQIA should be recorded on the IAR. A defined list of fields is detailed in Appendix 1. All fields must be completed.

4. Scope

4.1 This procedure applies to **all staff**. In this document, the term 'all staff' refers to regular full-time, regular part-time, contractors, consultants, agency and temporary employees. However, specific roles and responsibilities are documented within RQIA's Information Governance Policy, namely:

- The Senior Information Risk Owner (SIRO);
- The Information Asset Owners (IAOs); and
- The Information Asset Administrators (IAAs).

4.2 The Head of the Business Support Unit, supplemented by the BSO Data Protection Officer (DPO), will be responsible for reviewing the IAR, IFR and CRI for completeness and accuracy. They will also feedback any recommendations to the IAOs, as well as any perceived risks to the SIRO.

4.3 This procedure should be read in conjunction with relevant information governance policies.

5. Information Flow Register (IFR)

5.1 It is recognised that some information assets (for example, archived assets) may not have any inbound / outbound flows associated with them. This should be recorded on the IAR.

5.2 For **all** other information assets, all inbound / outbound flows should be recorded on the IFR. Equally, it is recognised that some information assets will have multiple inbound / outbound flows.

5.3 There should not be any flows that are not associated with an information asset.

5.4 A defined list of fields for the IFR is detailed in Appendix 2. All fields must be completed.

6. Corporate Records Inventory (CRI)

6.1 A records inventory has been used to describe a catalogue which holds details of all the records in existence within RQIA regardless of the format or media of those records.

6.2 It is recognised that some information assets (for example, archived assets) may not have any records associated with them. This should be recorded on the IAR.

6.3 For all other information assets, **all** records inventories should be recorded on the CRI. Equally, it is recognised that some information assets will have multiple records inventories.

6.4 There should not be any records within the CRI that are not associated with an information asset.

6.5 A defined list of fields for the IFR is detailed in Appendix 3. All fields must be completed.

7. Bi-Annual Assurance

7.1 As well as ensuring the IAR, IFR and CRI are kept up to date, IAOs will also be responsible for completing a bi-annual statement to confirm that their information assets are reviewed and that further assurances (such as access control and risk assessments) are provided. This will be issued via RQIA's Information Governance Group (IGG).

8. Information Risks

8.1 One of the most fundamental reasons for having an IAR is to document and mitigate information risks.

8.2 IAO's are responsible for assessing and documenting the risk associated with each of their information assets. The overall risk to each information asset should be calculated via assessment of the asset itself, as well as the flows and records associated with it, the documents security / safeguarding arrangements and any perceived weaknesses.

8.3 The overall risk score should be recorded against the information asset.

8.4 All information assets that are deemed to be 'medium' or 'high' are required to have an action plan put in place against them.

8.5 This action plan should be monitored. Any changes to the overall risk (i.e. where a risk is mitigated or reduced) should be reflected in the IAR in live time.

8.6 An action plan template is available in Appendix 6.

9. Review

9.1 This policy and any associated procedures will be reviewed no later than every 3 years, to ensure their continued relevance to the effective management of Information Governance within RQIA.

Appendix 1 – IAR Fields

Field	Defined Options	Description
IARN	None	This should be sequential for each Business Unit (and, where appropriate, teams). For example, Corporate Services assets will read: • CS/IA/ES/0001 (Estates) • CS/IA/IG/0001 (Info. Governance)
Asset_Name	None	The name of the information asset
Asset_Description	None	A brief description of what the asset is, and what business purpose it has
Business_Unit	Each BSO Business Unit is contained within this field	One business unit should be selected for each asset
Team	None	For larger business units, individual teams can be referenced here
Status	• Active • Inactive	Archived / defunct information assets should be recorded as 'Inactive'. All 'live' assets will be 'Active'
Asset_Type	• Information • Applications • Dataset • Other	Select one or more option to best describe the type of asset
Asset_Classification	• Confidential • Published • Unclassified	An asset will either contain publically available information, or will be confidential. Where neither has been selected, this will default to 'Unclassified'
Asset_Location	None	Describe the physical, virtual or electronic location(s) of the asset
Asset_Owner	None	The IAO should be a role, **not** a person
Asset_Adminstrator	None	The IAA should be a role, **not** a person
Access_Rights	None	List who sets access rights (this should be the IAA, and any other role who controls access rights)
Rights_Reviewed	• Yes • No	Record whether the IAO has reviewed access rights since the previous time the IAR was reviewed
Retention_Period	None	This should align with 'Good Management, Good Records[1]'

[1] https://www.health-ni.gov.uk/topics/good-management-good-records

Field	Defined Options	Description
Security_Measures	None	Briefly describe the security arrangements for this asset (for example: swipe card access, user access control, restricted folders, etc.). Examples may be: • Access Controlled / restricted • Locked physical storage • Secure offsite storage • Password protected • Permission-based • User access control *It should be noted that the above examples are neither prescriptive nor definitive. Staff completing the IAR should fully consider all relevant security measures per asset.*
Licenced	• Yes • No	Record whether the asset is licenced
Personal_Data	• Yes • No	Record whether the information asset holds any personal data
Legal_Basis	• 6(1)(a) - Consent • 6(1)(b) - Contract with data subject • 6(1)(c) - Legal obligation • 6(1)(d) - Protect vital interests of individual(s) • 6(1)(e) - Public interest / exercise of official duty • 6(1)(f) - Legitimate Interests	Select one (or more) legal basis.
Special_Category_Personal_Data	• Yes • No	Record whether the information asset holds any 'special categories' of personal data
Legal_Basis_Special_Category	• 9(2)(a) – Explicit consent • 9(2)(b) – Obligations under law • 9(2)(c) – Protect the vital interests of a data subject or another individual • 9(2)(e) – Personal data manifestly made public by the data subject • 9(2)(f) – The establishment, exercise or defence of legal claims • 9(2)(g) – Reasons of substantial public interest	Select one (or more) legal basis.

Field	Defined Options	Description
	• 9(2)(h) – Preventative or occupational medicine • 9(2)(i) – Reasons of public interest in the area of public health • 9(2)(j) – Archiving purposes in the public interest, or research or statistical purposes	
Flows_Mapped	• Yes • No	Have all inbound / outbound data flows been mapped on the IFR?
Shared_With	None	Detail who this asset (and/or its associated information) is shared with – both internal and external
Records_Documented	• Yes • No	Have all inbound / outbound data flows been mapped on the CRI?
Accounted_BCP	• Yes • No • N/A	Any information assets deemed to be business critical should be accounted for on BSO's Business Continuity Plan
Risks	None	Summarise all risks associated with this asset (this should incorporate all risks associated with individual flows and records attached to the asset). Examples may be: • Unauthorised access • Inappropriate disclosure • Lack of access / system access failure *It should be noted that the above examples are neither prescriptive nor definitive. Staff completing the IAR should fully consider all relevant information risks per asset.*
Risk_Impact	1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	Assign a risk impact, based on all information available
Risk_Likelihood	1. Rare (<5%) 2. Unlikely (5-20%) 3. Possible (21-50%) 4. Likely (51-95%) 5. Almost Certain (>95%)	Assign a risk likelihood, based on all information available

Field	Defined Options	Description
Risk_Grading	• Low • Medium • High • Extreme	Assign an overall Risk Grading, using the risk scoring matrix within RQIA's Risk Management Strategy, as well as Appendices 4 and 5 of this procedure
Action_Plan	None	If an action plan is required to mitigate / manage / tolerate (etc.) risk, summarise it here

Appendix 2 – IFR Fields

Field	Defined Options	Description
Flow_Description	None	A brief description of what the flow is
Asset_Link	None	This **must** be linked to the IARN within the Asset Register
Business_Unit	Each BSO Business Unit is contained within this field	One business unit should be selected for each asset
Team	None	For larger business units, individual teams can be referenced here
Bulk	• Yes • No	Record whether the information is transferred in bulk (for example, using FTP)
Flow_Type	• Inflow • Outflow • Both	Record whether the information is flowing in and/or out of the information asset
Outflow_Type	• Internal • External	Record whether the outflow is within BSO (Internal) or External
External_Location	• UK • EEA • OEEA • N/A	Record whether the information flows within the UK, within the EEA or outside the EEA.
External_Organisations	• None	List all external organisations the data flows to/from
Transfer_Method	• Automated via a secure network • Email • Fax • Hand Delivered • Posted • Removeable Media • Sent by Text Message • Up/Downloaded via a secure link	List the method(s) by which information is received / sent
Comments	None	This section should be used to highlight any perceived shortcomings (i.e. insecurity in transmitting information, etc.) which will be used to help inform the overall risk to the information asset

Appendix 3 – CRI Fields

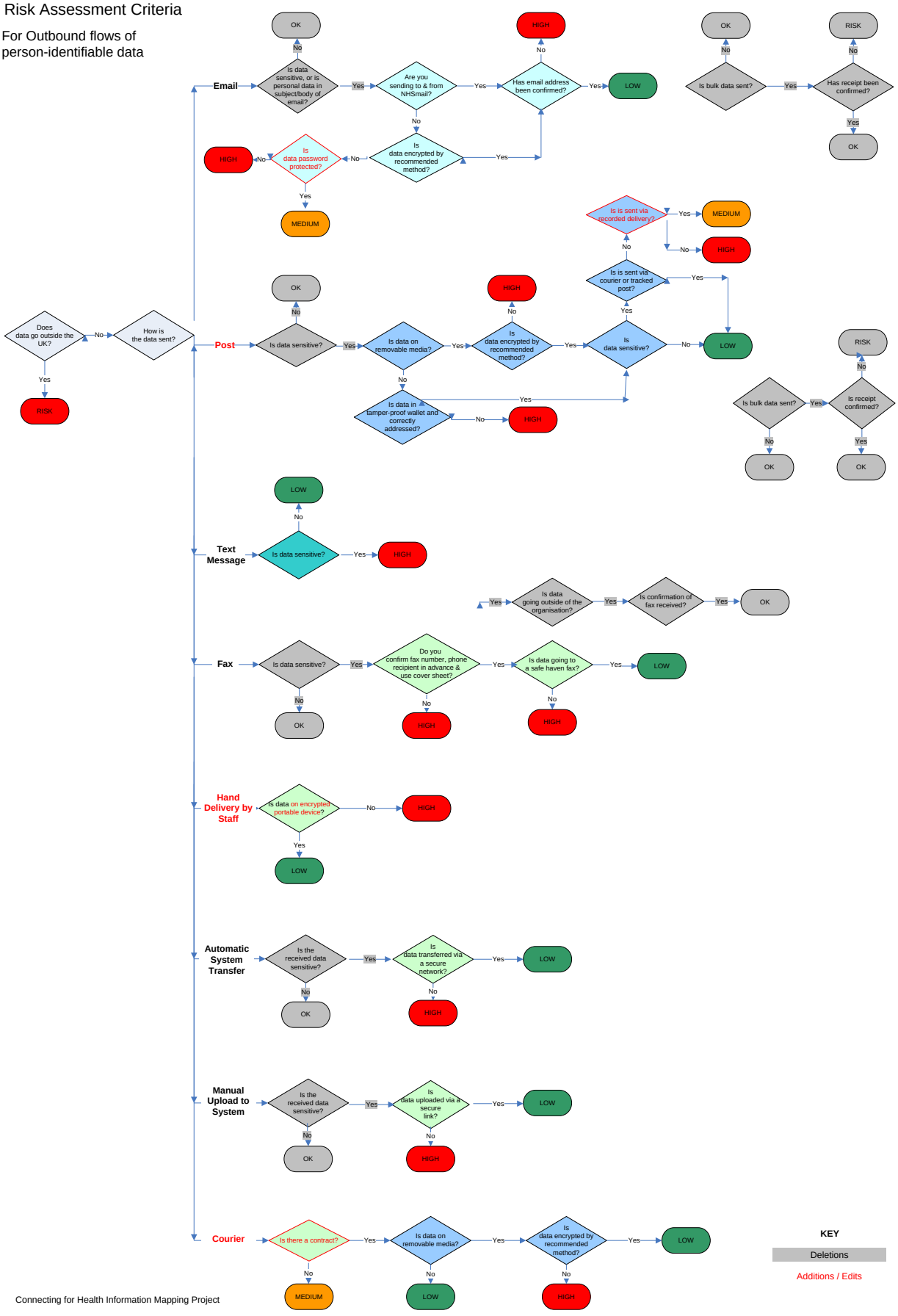
Field	Defined Options	Description
Record_Name	None	The name of the record collection
Business_Unit	Each BSO Business Unit is contained within this field	One business unit should be selected for each asset
Team	None	For larger business units, individual teams can be referenced here
Asset_Link	None	This **must** be linked to the IARN within the Asset Register
Record_Description	None	A brief description of what the record collection is
Confidential_Information	• Personal • Personal (Special Categories) • Corporate • None	Record what time of confidential information is held within the record collection
Who_Responsible	None	Detail who has overall responsibility for this record collection (NB: this is not necessarily the IAO). This should be a role, **not** a person.
Shared_Type	• Internal (Business Unit) • Internal (BSO) • External • None	Detail the category of stakeholder the record is shared with
Shared_External	None	If the record is shared outside of BSO, record who this is shared with
Records_Register	• Yes • No • N/A	Record whether a register of all records within the collection has been created and is maintained
Format	• Electronic • Manual	Record whether the record collection is manual and/or electronic
Manual_Stored	• Access Controlled Area • Locked Cabinet • Locked Carousel • Locked Desk • Locked Desk • Locked Office • Locked Room • Locked Safe	Record how the manual records are stored (multiple options are available). NB: where this is not specified, the default selection will be 'Unspecified Internal Storage'

Field	Defined Options	Description
	• Locked Store • Secure Offsite Storage • Unspecified Internal Storage • Website • Not Applicable	
Electronic_Stored	• Hard Drive • Network • Data Centre • Web hosted • Not specified • Not Applicable	Record how the electronic records are stored (multiple options are available). NB: where this is not specified, the default selection will be 'Not specified'
Sufficient_Storage	• Yes • No	Record whether there is sufficient physical and/or network space for current and future arrangements
Backup	• Yes • No	Record whether the records are backed up
Tracking_System	• Yes • No	Record whether there is a manual / electronic system to track records as they are moved
Last_Audited	• <6 months • <1 year • >1 year • Never	Detail when the records collection was last audited.
Further_Comments	None	This section should be used to highlight any perceived shortcomings (i.e. insecurity in transmitting information, etc.) which will be used to help inform the overall risk to the information asset.

Appendix 4 – Outbound Risk Assessment

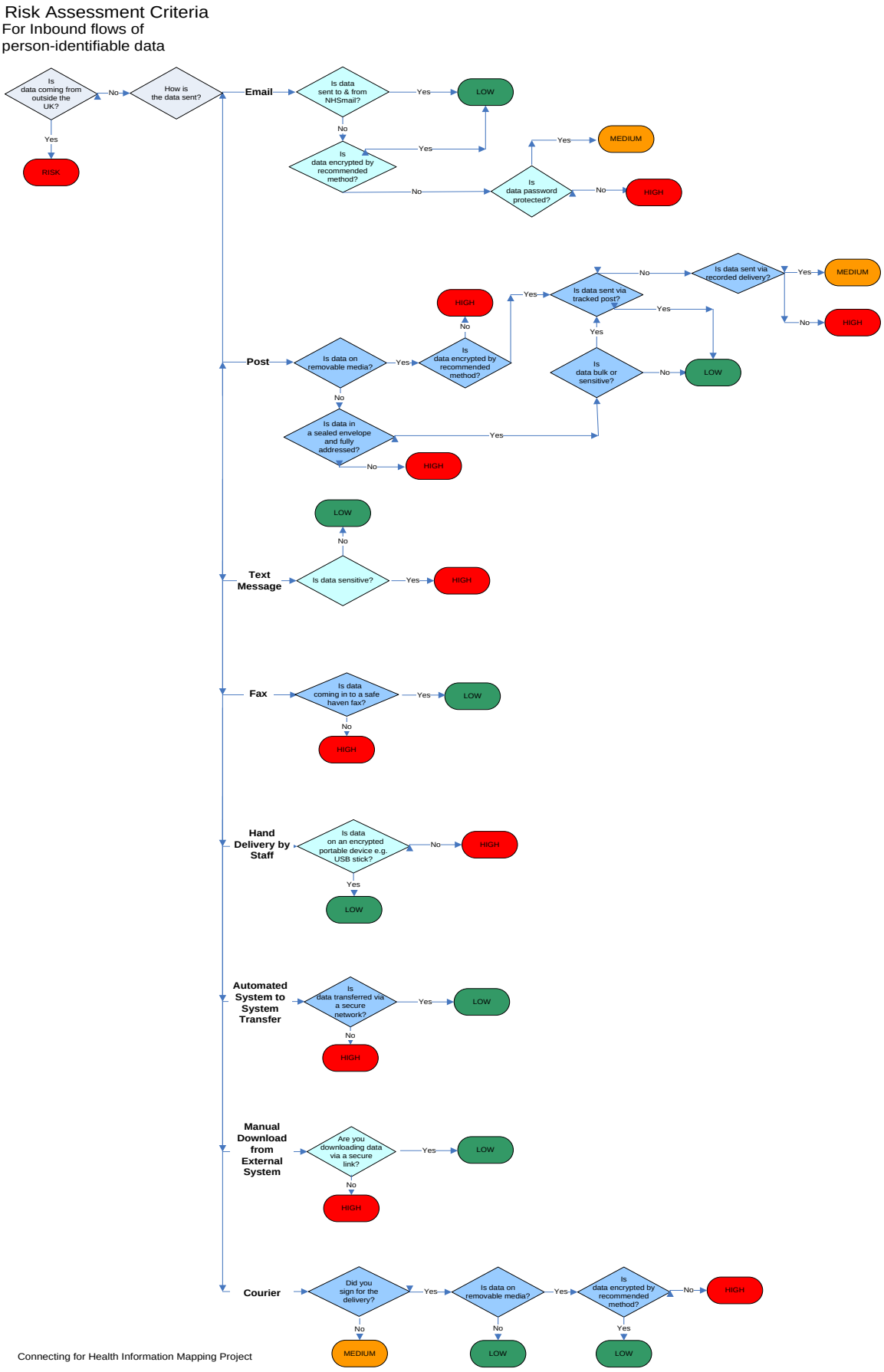
Risk Assessment Criteria

For Outbound flows of person-identifiable data



Connecting for Health Information Mapping Project

Appendix 5 – Inbound Risk Assessment



Appendix 6 – Information Risk Action Plan

Information Asset Name and IARN	
Information Asset Owner	
Business Unit	
Date of Assessment	

What is the threat? *(Please describe the threat of something damaging the confidentiality, integrity or availability of information)*

Examples of information asset threats may include:
Technical risks*: loss of essential service, technical failures, unauthorised access (inadequate password management), Data loss /corruption (disc error reports, lack of patching schedule)* ***Physical Risks:*** *Physical damage to asset, Unrestricted access to office, Security of laptops/removable media, Access to printouts,* ***Administrative Risks****; Inappropriate use of equipment (lack of policies), lack of user training, inaccurate management information* ***Service Provision Risks:*** *Corruption /inaccuracy of patient record, Failure to update patient records*

What are the consequences?

Examples of consequences may include:
Financial: *Negligent use / loss of patient data (inadequate security) – up to £500,000 issued by the Information Commissioner, Fine for copyright infringement, Additional cost of re-inputting data* ***Reputation****: Loss of reputation arising from a loss of patient data* ***Staff****: Lowering of staff morale/reduced quality of service*

Existing Controls

Current Risk

Impact:
Likelihood:
Grading:
Outcome (Accept / Treat):

Mitigation Plan

Action	Responsibility	Timescale	Revised risk score	Completion Data