GUIDANCE FOR INFORMATION ASSET OWNERS AND INFORMATION ASSET ADMINISTRATORS

Contents

1. Introduction

This document has been specifically written to support the Trust's information risk management framework and maintain appropriate protection of the Trust's information assets (IAs). In particular it will enable employees to identify an acceptable level of risk, beyond which escalation of risk management decisions is necessary. This guidance fits within the Trusts overall risk management framework.

All major IAs must be identified, have a responsible owner and maintenance responsibilities assigned to that owner. Accountability for IAs helps to ensure that appropriate information security measures are devised, implemented and monitored. Responsibility for implementing and managing controls may be delegated, although accountability must remain with the nominated owner of the IA.

.

Information risk management will not eliminate risk but will provide the structural means to identify, prioritise and manage information risks.

2. Background

The Information Governance (IG) Toolkit has been produced to assist organisations to achieve four fundamental aims of Information Governance.

These aims are:

- To support the provision of high quality care by promoting the effective and appropriate use of information
- To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools to support and enable them to discharge their responsibilities to consistently high standards
- To enable the organisation to understand its own performance and manage improvement in a systematic and effective way.

The IG Toolkit for Acute Trust's consists of 45 national requirements which cover all aspects of IG. In order to achieve compliance with the IG Toolkit, ownership and accountability for IAs needs to be assigned appropriately within the Trust and structured reporting arrangements should be documented and approved at Board level. The Information Asset Owner's (IAOs) and Information Asset Administrator's (IAAs) must actively risk assess information assets in order to provide regular reports and assurance to the Senior Information Risk Owner (SIRO).

The NHS information security management framework outlined in the Department of Health Information Security Management: Code of Practice outlines the requirements for high standards of management for all information assets, including patient records and other NHS corporate information, from potentially damaging threats, whether internal or external, deliberate or accidental.

3. Scope

The purpose of this document is to define the need for identifying information assets within the Trust, assigning ownership, and formalising the reporting structure for information risk management.

4. Information Assets

Information assets come in all shapes and forms but some of the component categories include:

- information / documents / processes
- software
- hardware / removable media
- services / knowledge

Key IAs are those that are central to the efficient running of departments within the Trust i.e. patient information, financial information, employee information, medicines management etc. IAs will also include the computer systems, network hardware and software which are used to process this data.

Non-computerised systems holding information must also be documented with relevant file identifications and storage locations.

There are four main categories of assets in the Trust:

I. Information Assets

Standard Operating Procedures
Policies / procedures
Training materials
Contracts and agreements
Business continuity plans
Databases
Archived information

II. Software Assets

Systems software (i.e. Microsoft windows)
Non-clinical systems (i.e. Electronic Staff Record)
Clinical systems (i.e. PAS, Orion, Ice)
Data encryption (i.e. Safe Boot, Endpoint)
Development and maintenance tools

III. Hardware / removable assets

Hardware assets - NHIS will be responsible for issuing hardware IAs and keeping a record of the equipment issued. No physical assets that have any capability for holding information can be purchased without involvement of NHIS. NHIS should be advised of new assets acquired through other routes and / or changes to existing assets.

Removable assets - i.e. data CDs / DVDs, llaptops, desktop personal computer (PC), portable hard drives, mobile phone / smart phone, memory stick, scanner, fax machine, iPad.

IV. Services assets

Access controls
People skills and knowledge

The service itself.

Please note: these lists are illustrative and not exhaustive.

5. Information Asset Register

IAs must be documented as part of the Trust's Information Asset Register (IAR); without which it would be impossible to implement the required controls across the Trust.

The IAR will be held by the Information Governance Team at SFH and maintained and populated by the Trust's nominated Information Asset Owners (IAOs) and Administrators (IAAs). The IAR will need to be updated regularly and submitted annually to the IG team in line with the requirements of the IG Toolkit.

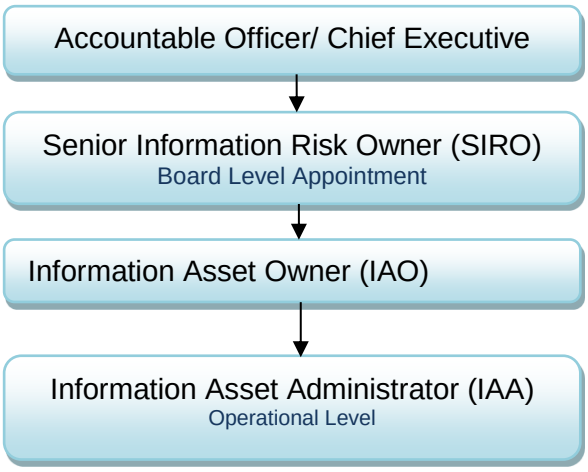
6. Information Flow Maps

The flow of an IA in and out of a department needs to be documented using the Trust's Information Flow Map (IFM).

The IFM is held by the Information Governance Team at SFH and is maintained and populated by the Trust's nominated IAOs and IAAs on a 6 monthly basis.

7. Key Roles and Ownership

There are four key roles required to ensure structured management arrangements for information risk:-



The Accountable Officer is the Chief Executive and has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks must be handled in a similar manner to other major risks such as financial, legal and reputational risks.

The SIRO who is also the Chief Financial Officer has been assigned responsibility for information risk at Board level. As an executive who is familiar with information risks and their mitigations; including risk assessment methodology, the SIRO provides briefings and reports to the Board on matters of performance and assurance.

IAOs are members of staff who are senior enough to make decisions concerning the asset(s) including to ensure information risk assessments are undertaken for all their information assets. At this Trust Information Asset Owners are Directors of Operations / Divisional Managers but can assign day to day responsibility for each information asset to an administrator or manager. Their role is also to provide assurance to the SIRO on the security and use of these assets.

IAAs provide support to their IAO by ensuring that policies and procedures are followed, recognising actual or potential security incidents /threats, consulting their IAO on incident management and ensuring that Information Asset Registers are accurate and kept up to date. There should be at least one IAA for each IAO and they are typically Service Leads / Line Managers / operational staff responsible for one or more information Assets.

8. Accountability

Each owner is accountable for the implementation and maintenance of IAs relating to their systems or work area. This role can be delegated to system management staff (IAAs). Each owner is responsible for ensuring that the relevant IAA is advised of any new assets or changes to existing assets, in order for the Information Asset Register to be updated accordingly. It is the responsibility of IAOs to put in place systems of communication and consultation which allow them, with their IAAs, to undertake the risk assessment, management and reporting to the standards outlined in the Toolkit.

9. Information Governance Toolkit Requirements relating to SIRO / IAOs / IAAs

Standard 110 - Formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.

The Senior Information Risk Owner and Information Asset Owners should ensure that contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

Standard 210 - All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements

Organisations should ensure that the implementation of new processes, services, systems and other Information assets does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements. It is vitally important that the impact of any proposed changes to the organisation's processes and/or IAs are assessed to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

Responsibilities and procedures for the management and operation of all Information assets should be defined and agreed by a senior person that leads on information risk (e.g. in the NHS, the *Senior Information Risk Owner* - SIRO and *Information Asset Owners* - IAOs).

The IAO (or equivalent) should ensure that documented procedures are in place governing the transfer of components from development to operational environments.

System software, hardware and operating procedures are subject to regular change.
It is essential that any changes are subject to a strict change management regime, to ensure that all changes are controlled and approved.

Standard 301 - A formal information security risk assessment and management programme for key Information Assets has been documented implemented and reviewed.

The Senior Information Risk Owner (SIRO) supported by Information Asset Owners (IAO)) is responsible for the identification, scoping definition and implementation of an information security risk programme to avoid gaps as far as is possible. The SIRO, IAOs and Information Governance forum (or its equivalent) and, ultimately, the organisation's Board (or equivalent) should be made aware of all information security risk assessments and approve identified risk mitigation plans.

Standard 305 - Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.

Organisations should control access to Information Assets and systems. This may be achieved by ensuring that system functionality is configured to support user access controls and by further ensuring that formal procedures are in place to control the allocation of access rights to local information systems and services. These procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

Each key information asset should have IG accreditation documentation that includes a system level security policy that contains rules regarding its access control. The system level security policy should be approved by the Information
Asset Owner (or individual with equivalent responsibilities), and Information Governance Board (or equivalent), be available to all users who are granted access to the system and should be reviewed on a regular basis.

The integrity and availability of information should be considered by the Information Asset Owner (e.g. system owner or individual with equivalent responsibilities). The 'need to know' principle of access should be supplemented with additional controls for altering or deleting information. File storage systems should be constructed with these criteria in mind as, in many cases, access to a folder allows the user to view, alter, copy or delete files in the folder (and sub-folders) unless they are protected.

The IAO should be identified in the system level security policy. The policy should also identify the need for and existence of a formal registration / deregistration procedure, with restricted authorisation for registering / deregistering users.

The IAO should ensure that effective procedures are in place for deregistering users who no longer need access to the system
For deregistration to work effectively the IAO and IAA should establish a formal agreement with the Human Resources department, to ensure the latter provides timely details of leavers and movers to the former.

The local Information Asset Owner should ensure a written procedure is developed to regularly review all system user access rights. The review should be used to ensure users

remain active and their access rights are allocated correctly. Six months is the recommended maximum period between such reviews.

Standard 307 - An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy.

The Senior Information Risk Owner (SIRO), who should be an Executive Director or other senior member of the Board should be allocated responsibility for owning information risk.

This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the organisation.

Standard 309 - Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place.

The *Information Asset Owner* (IAO) must analyse the effect that a disruption might have upon their business function (e.g. communications services) and link these to the overall Risk Policy to ensure these risks are incorporated into the organisation's corporate risk management and the overall direct and indirect consequences of disruption can be assessed and managed.

The Senior Information Risk Owner (SIRO) should ensure that a business continuity strategy is in place for all *critical information assets* and *critical processes*, including those provided under service contract or agreement by third parties.

A review group should be established by the IAO (or equivalent) to review, coordinate and test the BCP. A regular review and testing timetable should be established, with both being conducted on an annual basis at least.

Standard 310 - Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.

Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorised access to data and to protect against loss, damage, theft or compromise of Information Assets that would disrupt the organisation's activities. Consideration should also be given to equipment location.

Risk assessments should be carried out (see **requirement 301**) to assess these and other threats and establish suitable countermeasures. The Information Asset Owner (IAO)) should ensure that threats to services provided by third parties, or outsourced services, are taken into account within contracts and suitable controls and reporting procedures put in place. Information Asset Owners (or equivalent) should ensure that only authorised staff or contractors are allowed access to areas containing critical equipment. Printers, photocopiers and other equipment and supplies should not be stored within server rooms.

Standard 311 - Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.

Software and computerised information processing facilities are vulnerable to the introduction and spread of malicious code, such as computer viruses, network worms, Trojan horses, logic bombs and spyware. Users must be made aware of the dangers of unauthorised or malicious code. Information Asset Owners or those with equivalent responsibilities should ensure appropriate controls exist to detect or prevent its introduction or spread.

Standard 313 - Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.

The IAO should ensure there is a Network Security policy. IAOs responsible for information communication technology (ICT) networks, undertake reviews of information security risk in relation to those networks, and the controls and procedures required to mitigate these risks in accordance with the Network Security Policy.

Standard 323 - All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.

Organisations must ensure that all of their information assets that hold or are personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data.

An Information Asset Owner (IAO), or equivalent, should be assigned unique responsibility for each significant information asset, or group of assets, of the organisation. It is essential that each IAO understands the scope and boundaries of their assigned information assets, their approved purposes, who the users of the assets are and what their requirements for guidance and training may be, the criticality of the assets to the organisation, their dependency on other assets, and which other assets are dependent upon them. In order to achieve this detailed understanding, it is necessary that each information asset and its component parts are identified within an asset register.

IAOs should ensure that the IT Department and other departments that supply and maintain information processing equipment as components of their asset have relevant and approved procedures for the secure disposal of equipment that is no longer needed.

10. Disposal or Acquisition of an Information Asset

There must be a system in place to ensure that all acquisitions, disposals and transfers of IAs are identified and that the Information Asset Register is amended accordingly.

There should be:

- An IAA responsible for updating the relevant Information Asset Register
- A mechanism in place to ensure that the IAA is informed of all relevant acquisitions, transfers and disposals (i.e. the completion of a standard form)

- A process is in place in respect to recording and monitoring of work-in-progress and IAs in development.

11. Audit of Information Asset Register

In order to ensure the Information Asset Register remains current, accurate and complete it will be subject to regular audits and spot checks. IAOs should undertake regular reviews to manage the IG risks associated with their respective IAs.

12. Information Risk Assessments

Information risk assessments are required in order to ensure that threats, vulnerabilities and impacts are adequately accessed and included within the relevant risk register.

The SIRO will provide guidance to IAOs on the assessment method, format and frequency of risk assessments. The IAOs will submit the risk assessment results and associated mitigation plans (to include specific actions with proposed completion dates as well as an account of residual risks) to the SIRO for review.

The process of information asset risk assessments is supported by a programme of training for IAOs and IAAs

Guidance and templates for conducting risk assessments can be found on Appendix.

13. Training

All Trust staff are mandated to complete annual information governance training either at a face to face training session or Moodle.

The SIRO, IAO and IAA will be expected to complete additional training in relation to information risk via face to face training facilitated by the IG team or undertaking workbooks and assessments.

14. Data Privacy Impact Assessments

Projects that involve collecting personal information inevitably give rise to privacy concerns. A Data Protection Impact Assessment (DPIA) is a relatively new self-assessment process that has been developed by the Information Commissioner's Office (ICO) to help organisations to foresee the likely privacy impacts to individuals and to weigh these risks against the benefits to the public in the collection, use and secure disclosure of the information.

A DPIA helps to identify privacy risks, foresee problems and bring forward solutions. It is a process for evaluating a proposal to identify its potential effects upon individual privacy and data protection compliance; to examine how any detrimental effects might be overcome and to ensure that new projects comply with the data protection principles.

The Information Commissioner detailed guidance for undertaking PIA's provides organisations with a baseline for undertaking reviews and a procedure that meets legislative compliance.
(http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html).

15. Incident Reporting

Another important role for the IAOs and IAAs is to encourage the reporting of information governance and security incidents. This will enable the Trust to review information governance incidents for trends, patterns, impacts of controls in order to learn and adjust working practice as appropriate.

All IT security incidents and weaknesses including software malfunction should be reported immediately to the IT service desk. Other information related incidents should be reported to the information governance team using the Trust incident reporting system – DATIX. Examples of information related incidents include:

- Loss of and/ or malicious damage to hardware including computers, mobile phones, printers
- Computer virus attack
- Unauthorised software download and installation
- Vehicle break-ins or theft – where staff have been using the vehicle to carry patient records
- Misuse of access privileges including sharing of Smartcards or passwords
- Failure to log-out of hospital systems
- Unintended or unauthorised disclosure
- Unauthorised access to patient records or other information (paper or electronic)
- Unauthorised access to staff records
- Unauthorised access e.g.
    - by staff to hospital systems for unauthorised purposes
    - by the public\ patients over-hearing or seeing confidential information about others
- Insecure disposal of hardware or confidential material
- Non-compliance with Trust Internet and Email policies
- Unauthorised sharing of information with external agencies or the public
- Use of personal devices for Trust work instead of encrypted Trust devices
- Misuse of Trust equipment and resources such as faxes and Emails
- Sending faxes without adherence to the Safe Haven procedures
- Complaints from patients or a member of the public about breach of confidentiality
- Sharing of personally identifiable information by insecure Email

This list is illustrative and not exhaustive.

16. Appendices

APPENDIX ONE

Job Description

Job Title: **Senior Information Risk Owner (SIRO)**

Purpose of the Job:
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:

- Understand 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 the 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.

APPENDIX TWO

Job Description

Job Title: **Information Asset Owner (IAO)**

Purpose of the Job:
Information Asset Owners are senior individuals involved in running the relevant business.

The IAO's role is to:

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

Specific Responsibilities:

- Maintains understanding of 'owned' assets and how they are used
- Approves information transfers and assures the SIRO that these transfers are secure
- Approves and oversees the disposal mechanisms for the information asset when no longer needed
- Knows what information is held and who has access to it for what purpose
- Takes visible steps to ensure compliance with the Trust's Information Governance strategy and policies
- Undertakes quarterly reviews to document any IG risks associated with the information asset
- Understands and addresses risks to the information asset and provides assurance to the SIRO
- Receives, logs and controls requests from other staff for access to the information asset
- Ensures that changes to the information asset are documented with a formal sign off from the IG department following the undertaking of a Privacy Impact Assessment (if necessary).

APPENDIX THREE

Job Description

Job Title: **Information Asset Administrator (IAA)**

Purpose of the Job:
Information Asset Administrators will provide support to their IAO to:

- Ensure that IG policies and procedures are followed
- Recognise potential or actual security incidents and escalate
- Consult their IAO on incident management
- Ensure their information asset registers are accurate and up to date.

Specific Responsibilities:

- Maintenance of Information Asset Registers
- 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 appropriate IAO
- Report to the relevant IAO on the current state of the information 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 (Please refer to the Trust's Retention and Destruction of Records Policy for further information).