Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI202324/352
From: Other

Date: 31 October 2023

Subject: Information Asset Owner Structure

Q1 Do you have a single IAO for each information system or are they grouped for instance pathology, EPRs etc?

A1 Each system has its own designated information asset owner (IAO)

Q2 Do you have written duties / job description for them? If so please share

A2 We have written IAO responsibilities, which have recently been reviewed and are pending approval, see attached.

Q3 Do you have specific risk assessment documents? If so please share

A3 We don't have specific IAO risk assessment documents, systems are risk assessed via our data protection impact assessment (DPIA) process. DPIAs are completed for new systems and changes to systems or data processing.

Q4 Do your IAOs report to the SIRO or into another manager? Please provide a specimen structure

A4 The SIRO overseas IAOs via the Trust's information risk structure although they don't formally report to the SIRO, see below structure. This structure and our approach is based on the guidance that was issued by NHS Digital.

Q5 Do you assess all your systems at least annually?

A5 No, as above.

Q6 Do IAOs record risks directly into your risk register? If not who does?

A6 Yes, risks and actions identified during DPIAs are added to the overall project plan and to the appropriate corporate risk register.

Q7 Do all your IAOs have Information Asset Administrators (IAA)? Are your IAAs primarily Digital staff?

A7 IAOs will appoint as applicable, IAAs are not primarily Digital Systems staff.

Q8 If you have an EPR how many IAOs do you have for it? Could you supply the working role for each one.

A8 One - Associate Director for Operational IT.

Figure 1 – Information Risk Structure

Structural Model	LHCH Responsibility
Accounting Officer	Chief Executive
SIRO	Chief Digital and Information Officer
1+ Senior IAO	CSO, Divisional Head of Operations, Heads of Service, other senior responsible role
IAAs for each IAO	Operational staff responsible for one or more information assets identified in asset register
Information Asset Register	SIRO / Caldicott Guardian / CDIO / Head of Digital Systems / Cyber Manager / Head of IG & DPO / IG Manager / IG Team / CSO will ensure all assets are recorded

Information Asset Owner (IAO) Letter of delegated responsibilities

[date]

Dear [name],

I am writing to you as you have been identified from the Information Asset Register and your Divisional Lead as the owner of one or more Trust information assets (IAs) to outline your responsibilities and accountability as the designated information asset owner.

Information assurance is everyone's responsibility at Liverpool Heart and Chest Hospital NHS Foundation Trust, and your role as an Information Asset Owner (IAO) is critical to this objective and for ensuring security of our assets and the data within them.

IAOs are senior individuals nominated as owners of one or more Trust information assets, IAOs are required to understand and address risks to their information assets and provide assurance to the Trust's Senior Information Risk Owner (SIRO) on the security and use of assets.

The effective delivery of our services is dependent on effective information management. Information is a critical NHS resource; the loss, destruction or unauthorised access of information assets such as healthcare records could damage reputations and service delivery, and ultimately put patient care and safety at risk.

I am pleased to confirm your appointment as an IAO at Liverpool Heart and Chest Hospital NHS Foundation Trust for the following assets:

- [name of asset]
- [name of asset]
- [name of asset]

This letter formally sets out your responsibilities. You are granted delegated responsibility for ensuring that the IAO responsibilities as reflected in this letter and Appendix 1 are complied with.

In exercising this delegation, you are to ensure that you and all your team comply as appropriate with all formally approved policy and procedures, local and national. Particular attention is to be made to ensure that you:

- Understand the Trust's policies on the use of information and information risk management
- Ensure that all IAs 'owned' are accurately recorded in the Information Asset Register
- Maintain an understanding of 'owned' assets and how they are used
- Conduct annual risk assessment reviewed for all 'owned' information assets and ensure processes are in place to address these identified risks in line with the Trust's Information Risk Management Policy and relevant statutory and regulatory requirements
- Ensure appropriate identified training requirements are complied with relating to assets, asset administrators and users with access to or responsibilities in relation to the asset
- Provide an annual written assessment to the SIRO for all 'owned' assets covering all aspects of this responsibility have been undertaken and that you are confident that your area complies with policy, regulations and the law.

You may not make further sub-delegations of the role of IAO to other staff in your area, but it remains within your discretion as to how to implement elements of your IAO responsibilities within Liverpool Heart and Chest Hospital NHS Foundation Trust.

In support of your receipt of our formal delegation of this role we have registered you onto a GCHQ certified eLearning training module "Cyber Security for NHS Information Asset Owners". This will give you a clear guide to the role and responsibilities in an online format that is approx 45 mins long and can be completed either in one go or over a period of time for ease of completion.

Please confirm receipt of this letter by signing a copy and returning it to ITSecurity@alderhey.nhs.uk within three weeks from the date of issue of this letter.

Yours sincerely,

[name]
Senior Information Risk Owner

ACKNOWLEDGEMENT OF RECEIPT AND ACCEPTANCE

Acknowledged (signature):

Name:

Date:

Role:

Appendix 1: Liverpool Heart & Chest Hospital NHS Foundation Trust Information Asset Owner Responsibilities

The responsibilities of Information Asset Owners (IAOs) fall into four main categories:

Culture

- Lead and foster a culture that values, protects, and uses information as a strategic asset for the Trust and for public good
- Understand the SIRO's plans to achieve and monitor the right information security culture, and participate in that plan, including completing all required training
- Champion best practices to help ensure staff understand the importance of effective data security and protection.

Addressing risks

- Seek appropriate advice from designated Trust leads when reviewing risks to assets
- Ensure compliance with the provisions of UK data protection law and other relevant regulations / legislation
- Ensure that risks to data security and data protection are risk assessed via the Trust's Data Protection Impact Assessment (DPIA) process. DPIA should be carried out for all new projects that involve new or changes to existing personal data processing activities
- Ensure risks are reported in the suitable corporate risk register and where appropriate escalate risks to the SIRO

Understanding and managing assets and information flows

- Maintain an understanding of all 'owned' Information Assets (IAs) and how they are used. Maintain appropriate asset documentation such as System Level Security Policies (SLSPs)
- Approve data transfer from assets ensuring these are in line with business purposes and personal data disclosed is the minimum required for the purpose.
- Ensure all data transfers from assets are approved and comply with Trust policies and procedures to ensure proportionate security controls are applied to the transfer and subsequent storage of information.
- Ensure that data is securely returned or securely and permanently disposed of at the end of the data processing purpose.
- At end of life or decommissioning of assets, ensure both the asset and data within it are securely and permanently disposed of using approved disposal mechanisms.

Managing access

- Understand the Trust's policies on the use of information and information risk management
- Ensure all decisions regarding access to assets are made in accordance with UK data protection law and Trust policies
- Ensure access provided to an asset is the minimum required to meet business objectives
- Ensure assigned access and user-permissions are subject to regular review, minimum annually, and is supported by processes to remove access when user left the Trust or move between teams
- Ensure the use of the asset and access to it is checked regularly and records of checks maintained
- Ensure that user audit logs of asset access are held for a minimum of 6-months