care Information Exchange

Roles and Responsibilities

## Document Control

|  |
| --- |
| Revision History |
| Version | Date | Author / Editor | Details of Change |
| 1.0 | 29/07/2016 | Steve Janering | First Issue |

## Table of Contents

[1 Purpose of this document 1](#_Toc457564669)

[2 Information Asset Owner 2](#_Toc457564670)

[3 Privacy Officer 2](#_Toc457564671)

[4 Application Manager 3](#_Toc457564672)

# Purpose of this document

The purpose of this document is to provide participating organisations with a brief description of the role of Information Asset Owner. All participating organisations are required to have a nominated Information Asset Owner.

# Information Asset Owner

## Description

Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’. Information Asset Owners may be assigned ownership of several assets of their organisation. Every Information Asset must have an Information Asset owner. Where no information asset owner has been assigned the Information Asset Owner will default to the most relevant Divisional director of operations.

## Responsibilities

The role of the Information Asset Owner is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good.

In most cases the following tasks will be delegated by the Information Asset Owner to an appropriate Trust official:

* Registration & maintenance of the information assets on the Information Asset Register
* Carry out a formal information security risk assessment for all Information Assets they own to ensure all threats, vulnerabilities and impacts are properly assessed and where appropriate included in an organisation-wide risk register
* Put in place a System Specific Security Policy that should control access to Information Assets 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 lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. Special attention should be given to managing access rights which allow support staff to override system controls.
* Ensure Business continuity plans are up to date and tested for all critical information assets
* To document and adequately protect transfers / flows of information, organisations need to identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with professional standards and relevant legislation (e.g. Principle 7 of the Data Protection Act 1998 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data).

# Privacy Officer

(This description is based on functionality which is currently under development by the Care Information Exchange system suppliers (Patients Know Best).

## Description

Within the Care Information Exchange, users view records by creating a legitimate relationship and / or requesting permission to view. System alerts are generated when a permission to view is over-ridden (“Emergency Access”).

The Privacy Officer then investigates and manages alerts using the Care Information Exchange system. The CIE enables Privacy Officers to audit viewing activity using CIE audit reporting functionality.

The Privacy Officer role can be specifically for the purpose of CIE or incorporated into the existing IG function of an organisation.

## Responsibilities

The Privacy Officer should:

* Routinely review list of alert notifications within CIE.
* Investigate alerts e.g. identifying unusual patterns of Emergency Accesses.
* Escalate inappropriate accesses to the NWL Digital Governance Group.
* Ensure local IG processes incorporate CIE viewing activity e.g. Information Governance Policy, Confidentiality Policy.
* Follow policy outlined in CIE Incident Management Protocol, including:
	+ Notify NWL Digital ISA Incident Management Security Officer of any security incident.
	+ Notify the NWL Digital ISA nominated Partnership Incident Management Security Officer of any local security incident which has an effect upon any member of the NWL Digital partnership, such as security compromise.

Emergency Access alerts will identify the patient whose record has been viewed and the user that has viewed the record. Alert notifications cannot be switched off and should be reviewed on a regular routine basis for monitoring and investigation. Each organisation must ensure that they have a nominated responsible officer (normally the Privacy Officer), with the correct CIE access to manage the alert process.

# Application Manager

## Description

Depending on the scope and extent of CIE use within an organisation the application manager role may be taken on as a small part of an existing role, or may require the equivalent of a whole time role which could be divided amongst several people. Over time as the CIE is deployed more extensively throughout NW London there may also be a requirement for a central team of resources to perform this role.

## Responsibilities

* Manage new starters and leavers to the organisation “umbrella team” and any departmental “specialty teams” which are in use within the organisation. This will include processing formal requests from staff managers and creating and removing staff accounts to access the system.
* Reset passwords for staff users where appropriate ID has been provided.
* Schedule and complete regular day to day application administration/housekeeping tasks and procedures.
	+ Gain a thorough understanding of the supported application software so as to be able to administer and support the application.
	+ Monitor the performance of the system and take appropriate action or advise if escalation is required to improve performance.
	+ Ensure monitoring output is reviewed and trends are recorded and escalated where appropriate.
	+ Own and manage calls logged on the local ICT helpdesk relating to CIE.
	+ Triage issues and resolve or escalate as appropriate.
	+ Provide support and advice on a corporate basis to all levels of staff relating to CIE enquiries.
	+ To develop and foster good working relationships with the system vendors (Patients Know Best) and any third party contractors associated with the system.
	+ Ensure that changes are made in a timely manner and in the prescribed order to ensure integration integrity with other systems is maintained.
	+ Maintain accurate records of changes to reference data.
	+ Investigate and resolve issues of inaccurate or incorrectly mapped reference data ensuring issues are escalated to all affected parties.
	+ Ensure all clinician led categorisation of data (general, mental, sexual and social) are reflected in the system messaging and display within CIE.
	+ Ensure clinician led configurable patient delays are accurately represented within CIE e.g. 4 week delay to release of sensitive pathology results to patients.
	+ Through a combination of knowledge transfer and training initiatives ensure that there exists an adequate level of knowledge/skills within local teams to maintain systems when other team members are unavailable.
	+ Ensure business continuity plans are kept up-to-date.
	+ Advise of issues that should be included in the CIE project risk log.

## Data corrections

The intention is that where system integration is in place, the majority of data corrections should be automated through system to system messaging. However, there will be cases such as erroneous record merges which then require separation, which will not be corrected through automated system messaging.

In these cases, which can be highly complex, local processes will need to be established which ensure that any data corrections performed on source systems are also reflected in the CIE system.

Over time this is expected to require co-ordination between organisations and will be further defined as the CIE project develops.