

Document Details		
Title	IG06 Assignment of Information Governance Responsibilities	
Author	CIC Board	
Quay Primary Healthcare CIC ref no:	IG06	
Version	1.4	
Approval process		
Approved by	CIC Board	
Date approved	May 2018	
Lead Director	Medical Director	
Category	Information Governance	
Sub Category	Risk Management	
Next Review Date	14 February 2024	
Superseded document (If applicable)		
Distribution		
Who the policy will be distributed to	All Quay Primary Healthcare CIC Team	
Method	Email and Team Net	
Version Control		
No:	Date	Amendment
1.1	16 May 2020	Policy review and revision – change of organisation name
1.2	30 Nov 2020	Adopted MLCSU policy (new IG provider for WPC CIC Nov 20)
1.3	25/11/2021	Change of organisation name - Quay Primary Healthcare CIC
1.4	14/02/2023	Labelled and tidied document, no content changes made
1.5		
1.6		
1.7		

Quay Primary Healthcare CIC

Assignment of Information Governance Responsibilities

Amy Cannon is overall Information Governance (IG) Lead for Quay Primary Healthcare CIC and will work in collaboration with Dr Quincy Chuka who will lead on Caldicott, Data Protection and Freedom of Information issues

A: Information Governance Lead

As Information Governance Lead, Amy Cannon will:

- Ensure that IG is regularly discussed in Strategic Management Team meetings
- Ensure the development of an Information Governance (IG) Policy that sets out at a high level the organisation's intended approach towards IG
- Ensure the development of an Information Governance Strategy that sets out how the IG Policy will be supported in terms of resources and implementation, and coordinate all/any staff within Quay Primary Healthcare CIC who are given specific data protection, confidentiality and Freedom of Information responsibilities
- Ensure that all staff are familiar with and implement the policies and processes adopted by Quay Primary Healthcare CIC to ensure compliance with IG-related legislation and best practice guidance
- Take the lead in raising awareness of the importance of Information Governance throughout Quay Primary Healthcare CIC and encourage all staff that hold, obtain, record, use and share information to participate in raising IG standards
- Ensure that an annual assessment of Quay Primary Healthcare CIC's performance against the Requirements in the Information Governance Toolkit is completed and submitted
- Ensure that an IG plan is in place for each Requirement to enable sustainability or improvements to be made against the assessment by setting targets to reach the next level
- Ensure policies and procedures are reviewed on an annual basis and arrange for amendment as necessary
- Ensure that all systems and processes are secure and compliant with the legislation and best practice guidance and identify any current/potential risks and mitigate against them where appropriate
- Ensure that Quay Primary Healthcare CIC Business Continuity Plan adequately covers IG aspects of any interruption to service whether technical or practical
- Ensure the public are aware of their rights under the Data Protection Act 2018, General Data Protection Regulations and the Freedom of Information Act 2000, and how Quay Primary Healthcare CIC is handling their information for different purposes
- Ensure that all staff whether working on a permanent, temporary or casual basis for Quay Primary Healthcare CIC or contracted to Quay Primary Healthcare CIC sign appropriate confidentiality clauses as part of their contract or if working on an ad hoc basis, before being given access to the premises/ information

- Act as Quay Primary Healthcare CIC Registration Authority (RA) Lead and develop a plan/procedure to monitor and enforce compliance with the Terms and Conditions of NHS Smartcard usage. (304 1a)
- Ensure that Quay Primary Healthcare CIC creates and continually reviews an up-to-date Information Asset Register (316 1a)
- Monitor Quay Primary Healthcare CIC's information handling activities to ensure compliance with the law and best practice guidance
- Ensure that each staff member receives IG training as part of the new starters' Induction Programme and completes mandatory IG refresher training at least annually thereafter to ensure knowledge is kept up to date
- Undertake a training needs analysis for all staff to identify additional training required for a specific job role and ensure that this is provided and completed
- Ensure personal IG knowledge is kept up to date
- Assist with investigations into complaints/ reports about breaches of confidentiality, the Data Protection Act 2018, General Data Protection Regulations or Freedom of Information Act 2000, and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions
- Provide reports to Quay Primary Healthcare CIC management relating to progress towards completion of the improvement plan and any potential risks to Quay Primary Healthcare CIC.
- Provide advice to Quay Primary Healthcare CIC on Information Governance issues and access to expert/legal advice when necessary
- Support monitoring visits from the commissioning or other monitoring organisations as appropriate

B: Caldicott Guardian

As Caldicott Guardian, Dr Quincy Chuka will:

- Act as the 'conscience' of Quay Primary Healthcare CIC by actively supporting work to facilitate and enable information sharing whilst advising on options for lawful and ethical processing of information as required
- Champion Information Governance requirements at team level and reflect patient's interests regarding use of patient identifiable information in management discussions
- Ensure, in collaboration with the Information Governance Lead, that confidentiality issues are appropriately reflected in organisational policies and working procedures for staff
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with bodies both within and outside the NHS. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related new IT systems, disclosure to research interests and disclosure to the police
- Be consulted where necessary on information requests, typical examples being:
 - a request from the police for access to patient information
 - requests from patients to delete information from their records
 - an actual or alleged breach of confidentiality
- Ensure that appropriate Caldicott Guardian training is completed and updated to ensure skills are kept up-to-date with changes in legislation and best practice guidance

C: Senior Information Risk Owner (SIRO)

As Senior Information Risk Owner, Lorraine Stratulis will:

Lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its customers

- to ensure the Organisation has a plan to achieve and monitor the right NHS IG culture, across the Organisation and with its business partners
- to take visible steps to support and participate in that plan (including completing own training)
- to maintain sufficient knowledge and experience of the organisation's business goals with particular emphasis on the use of and dependency upon internal and external information assets
- to ensure the Organisation has Information Asset Owners (IAOs) who understand their roles and are supported by the information risk management specialists that they need
- to initiate and oversee an information risk awareness / training programme of work to communicate importance and maintain impetus
- to ensure that good information governance assurance practice is shared within the organisation and to learn from good practice developed and practiced within NHS organisations locally and nationally

Own the organisation's overall information risk policy and risk assessment processes and ensure they are implemented consistently by IAOs.

- to act as the focal point for information risk management in the organisation including resolution of any pan-organisation or other escalated risk issues raised by Information Asset Owners, Information Security Officers, Auditors etc
- to develop and implement an IG Information Risk Policy that is appropriate to all departments of the organisation and their uses of information setting out how compliance will be monitored
- to initiate and oversee a comprehensive programme of work that identifies, prioritises and addresses NHS IG risk and systems' accreditation for all parts of the organisation, with particular regard to information systems that process personal data
- to ensure that Privacy Impact Assessments are carried out on all new projects when required in accordance with the guidance provided by the Information Commissioner
- to review all key information risks of the organisation on a quarterly basis and ensure that mitigation plans are robust
- to ensure that NHS IG Policy, information risk management method and standards are documented, applied and maintained consistently throughout the organisation's information governance risk assessment and management framework
- to ensure that information risk assessment is completed on a quarterly basis taking account of extant NHS Information Governance guidance as required by the IGT.
- to understand the information risks faced by the organisation and its business partners ensuring that they are addressed, and that they inform investment decisions including outsourcing
- to ensure that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny

Advise the accounting officer on the management of information risk and provide assurance

- to ensure routine meetings are established with the organisation's Chief Executive or Accounting Officer to brief, discuss or report upon matters on information governance risk assurance and information risk culture affecting the organisation, including input to the annual NHS IG reporting processes

- to sign off an annual assessment of performance, including material from the IAOs and specialists,
- covering NHS Information Governance reporting requirements

Own the organisation's information incident management framework

- to ensure that the organisation has implemented an effective information incident management and response capability that supports the sharing of lessons learned
- to ensure that there is a considered and agreed IG incident response and communications plan available, including the reporting of 'perceived' or 'actual' Information Governance Incidents.
- to ensure that the organisation's management, investigation and reporting of IG Incidents conforms to national guidance and does not conflict with the organisation's policies and procedures for non-IG Incidents

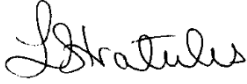
D: Data Protection Officer

MLCSU IG is the named Data Protection Officer.

The Data Protection Officer will:

- Inform and advise the organisation and employees about obligations to comply with the General Data Protection Regulations and other data protection laws
- Monitor compliance with the General Data Protection Regulations and other data protection laws, and with your data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits
- Advise on, and to monitor, data protection impact assessments
- Cooperate with the supervisory authority
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)
- operate independently and not dismissed or penalised for performing their tasks

Names and Signatures

Name	Role	Signature
Amy Cannon	Data Protection Officer IG Lead	
Dr Quincy Chuka	Caldicott Guardian	
Lorraine Stratulis	Senior Information Risk Owner	
Mark Dyson	Chief Executive Officer	