Information Governance & Data Security and Protection Policies

Quay Primary Healthcare CIC

Document Details	
Title	**IG00 Information Governance & Data Security and Protection Policies**
Author	CIC Board
Quay Primary Healthcare CIC ref no:	IG00
Version	1.5

Approval process	
Approved by	CIC Board
Date approved	May 2018
Lead Director	Medical Director
Category	Information Governance
Sub Category	Risk Management
Next Review Date	July 2025
Superseded document (If applicable)	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	Updated Caldicott Principles, work needed on FOI publication on website
1.5	01/07/2025	Policy Review
1.6		
1.7		

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Quay Primary Healthcare CIC will establish and maintain this policy and the associated procedures to ensure compliance with the requirements contained in the Data and Security Protection Toolkit (DSPT).

This policy and its supporting procedures are fully endorsed by the Senior Management Team through the production of these documents and their endorsement and approval by the Information Governance Lead and Caldicott Guardian.

1. Scope

This policy covers all aspects of information within the organisation, including but not limited to:

- Patient/client/service user information
- Personal Information
- Organisational Information

This policy covers all aspects of handling information, including but not limited to:

- Structured record systems – paper and electronic
- Transmission of information – email, other forms of electronic transmission such as FTP, post and telephone

This policy covers all information systems purchased, developed and managed by or on behalf of Quay Primary Healthcare CIC, and any individual directly employed or otherwise working for Quay Primary Healthcare CIC.

The key component underpinning this policy is the annual improvement plan arising from a baseline assessment against the standards set out in the Data Security and Protection Toolkit.

This policy cannot be seen in isolation as information plays a key part in corporate governance, strategic risk, clinical governance, Caldicott principles, service planning, performance and business management.

The policy therefore links into all these aspects of Quay Primary Healthcare CIC and should be reflected in any respective strategies/policies.

2. Principles

Quay Primary Healthcare CIC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

All staff should read and sign the Staff Confidentiality Agreement and a copy should be retained on the staff record.

Quay Primary Healthcare CIC fully supports the principles of corporate and information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Quay Primary Healthcare CIC also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Quay Primary Healthcare CIC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in Quay Primary Healthcare CIC to ensure and promote the quality of information and to actively use information in decision making processes.

Quay Primary Healthcare CIC will abide by the Caldicott Principles – these are listed in **Appendix A**, and the Data Protection Act 2018 principles – these are listed in **Appendix B**

There are 5 key interlinked strands to the Information Governance Policy:

- Openness
- Legal Compliance
- Information Security
- Records Management
- Data Quality

2.1 Openness

- Quay Primary Healthcare CIC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Non-confidential information about Quay Primary Healthcare CIC and its services will be available to the public through a variety of media (e.g. leaflets, Internet, newsletter).

- Quay Primary Healthcare CIC regards all identifiable information relating to patients as confidential. Compliance with legal and regulatory framework will be achieved, monitored and maintained.
- Quay Primary Healthcare CIC regards all identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- Quay Primary Healthcare CIC will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, Common Law Duty of Confidence, Freedom of Information Act 2000 and Environmental Information Regulations.
- Quay Primary Healthcare CIC will ensure that when personal identifiable information is shared, the sharing complies with the law, guidance and best practice and both service users' rights and the public interest are respected.
- Information Governance training including awareness and understanding of Caldicott principles and confidentiality, information security, records management and data protection will be mandatory for all staff. Information governance will be included in induction training for all new staff
- Quay Primary Healthcare CIC will undertake annual assessments and audits of its policies and arrangements for openness.
- Patients will have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- Quay Primary Healthcare CIC will have clear procedures and arrangements for liaison with the press and broadcasting media.
- Quay Primary Healthcare CIC will have clear procedures and arrangements for handling queries from patients and the public.

2.2 Legal Compliance

- Quay Primary Healthcare CIC regards all person identifiable information, including that relating to patients as confidential.
- Quay Primary Healthcare CIC will undertake annual assessments and audits of its compliance with legal requirements.
- Quay Primary Healthcare CIC regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- Quay Primary Healthcare CIC will ensure that data is stored securely and processed in line with relevant legislation in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.
- Quay Primary Healthcare CIC will ensure compliance with the Data Protection Act 2018, Human Rights Act 1998 and the Common Law of Confidentiality and other relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

2.3 Information Security and Incident Reporting

- Quay Primary Healthcare CIC will undertake annual assessments and audits of its information and IT security arrangements through the Data Security and Protection Toolkit framework.
- Quay Primary Healthcare CIC will promote effective confidentiality and security procedures to its staff through policies, procedures and training.
- Quay Primary Healthcare CIC will ensure that data is stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures
- Quay Primary Healthcare CIC will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- Quay Primary Healthcare CIC will log and record all reportable data security and protection incidents via the Data Security and Protection Toolkit reporting tool.
- Quay Primary Healthcare CIC will report a notifiable breach to the Information Commissioner's Office without undue delay, if longer than 72 hours then a specific reason for the delay will be given.

2.4 Records Management

- Quay Primary Healthcare CIC will undertake annual assessments and audits of its records management arrangements.
- Quay Primary Healthcare CIC will ensure that information is managed throughout its lifecycle of creation, retention, maintenance, use and disposal.
- Quay Primary Healthcare CIC will ensure that information is effectively managed so that it is accurate, up to date, secure, retrievable and available when required.
- All staff have a duty for the maintenance and protection of records they use. Only authorised staff should have access to records.
- Quay Primary Healthcare CIC will identify and safeguard vital records necessary for business continuity and should include them in the business continuity /disaster recovery plans.
- Quay Primary Healthcare CIC will record any incidents relating to records, including the unavailability and loss on the Data Security and Protection Toolkit.
- Accuracy of statements i.e. record keeping standards, should pay particular attention to stating facts not opinions.
- Quay Primary Healthcare CIC will periodically check for records that have reached their minimum retention period and if there is no justification for continuing to hold them, they will be disposed of appropriately.

2.5 Data Quality

- It is the responsibility of all staff to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner. The quality of information produced can have a significant impact on the quality of services that we provide.
- Quay Primary Healthcare CIC will ensure the quality of their records to the highest standards and wherever possible, information quality should be assured at the point of collection.

Quay Primary Healthcare CIC will ensure:

- That all data must be correct and accurately reflect what happened. However, it is important to note that the accuracy and timeliness of data does not just relate to patients.
- That data will be within an agreed format which conforms to recognised national or local standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.
- That data will be captured in full. All mandatory data items within a data set should be completed and default codes will only be used where appropriate, not as a substitute for real data.
- That data will be dealt with in a timely manner and should be collected at the earliest opportunity; recording of timely data is beneficial to the treatment of the patient. All data will be recorded to a deadline which will ensure that it meets national reporting and extract deadlines.
- That data collected should be understood by the staff collecting it and data items should be internally consistent. Data definitions should be reflected in procedure documents.
- That data will reflect the work of Quay Primary Healthcare CIC and not go unrecorded.
- That patients should not have duplicated or confused patient records, and where possible data should be recorded once, and staff should know exactly where to access the data. Where a duplicate record is created, for example in the event that a record is misplaced, records should be merged once the original is found.

3. Responsibilities

Amy Cannon the designated Information Governance Lead in Quay Primary Healthcare CIC, is responsible for overseeing day to day Information Governance issues: developing and maintaining policies; standards, procedures and guidance; co-ordinating Information Governance in Quay Primary Healthcare CIC; raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the Information Governance responsibilities incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

Dr Quincy Chuka has been appointed as Caldicott Guardian for Quay Primary Healthcare CIC. This role is an amalgamation of management and clinical issues which helps to ensure the involvement of healthcare professionals in relation to achieving improved information governance compliance. The

Caldicott Guardian has responsibility for ensuring that all staff comply with the Caldicott Principles and the guidance contained in the NHS Digital document – "A Guide to Confidentiality in Health and Social Care".

The Caldicott Guardian will guide Quay Primary Healthcare CIC on confidentiality and protection issues relating to patient information. This role is pivotal in ensuring the balance between maintaining confidentiality standards and the delivery of patient care. The Caldicott Guardian will also advise
Quay Primary Healthcare CIC Management Team on progress and major issues as they arise.

MLCSU IG has been appointed as Data Protection Officer. The role will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Full details of the roles and responsibilities for named individuals can be found in the document – Assignment of Responsibilities.

4. Training /Awareness

Information governance will be a part of Quay Primary Healthcare CIC'S induction process. Records of all inductions will be retained on staff records.

All new and existing staff will receive annual mandatory training and guidance on information governance, which will include coverage of Caldicott and confidentiality, data protection, information security and Freedom of Information to ensure that staff are aware of their responsibilities for: the confidentiality of the information they handle; situations where it is appropriate to disclose information to persons other than the patient; safe haven procedures; quality record keeping; secure storage and disposal of information.

All staff must undertake the Data Security Awareness Level 1 e-learning module or equivalent training, and an assessment should be completed to demonstrate the required knowledge and understanding and to complete the training. This can be accessed through the E-Learning for Health website: https://www.e-lfh.org.uk/programmes/data-security-awareness

Annually all staff will complete Information Governance Refresher Training. Records of the staff compliance with training will be kept and monitored and the evidence from the training will be used to support the submission of the Data Security and Protection Toolkit.

5. Individual Rights

Individuals legally have rights in relation to the data that is processed about them. Quay Primary Healthcare CIC must have processes in place should an individual choose to exercise any of their rights. It is vital that all staff can recognise such requests to allow them to be processed within the timescales set out in law.

5.1 Subject Access Requests

Quay Primary Healthcare CIC will log and record all Subject Access Requests that are received in line with the Data Protection Act 2018.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Fax
- Post
- Social media
- Practice website

Where an individual is unable to make a written request, it is the Department of Health's view that in serving the interest of patients it can be made verbally, with the details recorded on the individual's file.

All requests will be dealt with within one month, as per the legislation.

All information is to be supplied free of charge (although "reasonable" fees can be charged for an excessive request or for further copies).
A request may be received for information relating to a deceased individual. In this case certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

• The patient's personal representative (Executor or Administrator of the deceased's estate)
• Any person who may have a claim arising out of the patient's death

A Next of Kin has no automatic right of access, but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records.

The Common Law Duty of Confidentiality extends beyond death.

5.2 Right to erasure

The right to erasure is also known as 'the right to be forgotten' and means that individuals have the right to have personal data that Quay Primary Healthcare CIC holds about them erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If the individual withdraws their consent for Quay Primary Healthcare CIC to process their data (if this was the basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data has to be erased in order to comply with a legal obligation.

The Right to Erasure will be reviewed on a case by case basis and will be limited if the information has been processed for the purpose of providing direct care to the individual.

5.3 Right to be informed

Individuals have the right to be informed of the processing Quay Primary Healthcare CIC undertakes with their personal data. Quay Primary Healthcare CIC will information all individuals via their Privacy Notice.

The Privacy Notice is available on Quay Primary Healthcare CIC website www.warringtonhealthplus.org

5.4 Right to rectification

If personal data that Quay Primary Healthcare CIC holds is found to be inaccurate or incomplete, individuals have the right to have it rectified. This includes any data that Quay Primary Healthcare CIC may have passed on to others unless this proves impossible or involves disproportionate effort. If this is the case, Quay Primary Healthcare CIC will explain to the individual why this has not been possible.

The individual can make a request for rectification either verbally or in writing and Quay Primary Healthcare CIC has one calendar month to respond to such requests. The right to rectification is not absolute and Quay Primary Healthcare CIC has the right to review the request to see if it can be complied with.

Requests which are deemed to be unfounded, excessive, repetitive in nature or required to be maintained legally may be refused.

5.5 Right to restrict processing

Individuals have the right to restrict processing in certain situations. The data can still be retained by Quay Primary Healthcare CIC; however, certain restrictions can be applied.

The situations where processing restrictions may apply are:

- If the individual contests the accuracy of the data Quay Primary Healthcare CIC hold about them, Quay Primary Healthcare CIC will restrict the processing until the accuracy of the data has been verified;
- If Quay Primary Healthcare CIC is processing the individual's data as it is necessary for the performance of a public interest task and the individual has objected to the processing, Quay Primary Healthcare CIC CIC will restrict processing while they consider whether their legitimate grounds for processing are overriding.;

- If the processing of the individual's personal data is found to be unlawful but they oppose erasure and request restriction instead; or
- If Quay Primary Healthcare CIC no longer need the data held about the individual, but the individual requires the data to establish, exercise or defend a legal claim.

Requests can be made verbally or in writing to Quay Primary Healthcare CIC and Quay Primary Healthcare CIC will respond within one month.

5.6 Right of data portability

Individuals have the right to request a copy of their data in a portable format if the processing of the personal data is on the legal basis of consent. If the personal data is being processed for the purpose of providing direct care to the individual, then this right will not apply.

5.7 Right to object

Individuals have the right to object to their data being processed if the data is being processed for the performance of a task in the public interest or exercise of official authority.

All objections will be reviewed on an individual basis and objections can be made to Quay Primary Healthcare CIC both verbally or in writing.

5.8 Right to object to automated decision making and profiling

Any information processed by Quay Primary Healthcare CIC which has been automated, meaning without human involvement will be eligible for this right.

Quay Primary Healthcare CIC does not currently use automated decision making or profiling tools.

6. National Data Opt-Out

All health and care organisations must comply with the national data opt-out policy by March 2020.

Quay Primary Healthcare CIC complies with the national data opt-out policy and the use of the technical services to check for national data opt-outs in line with technical specifications and instructions.

Quay Primary Healthcare CIC ensures that if patients do not wish for their confidential patient information to be used for research and planning, they can choose to opt out securely online or through a telephone service by contacting Quay Primary Healthcare CIC directly. Further details are made available to the public via the Privacy Notice on our website. (www.warringtonhealthplus.org)

7. Freedom of Information Requests

Quay Primary Healthcare CIC will deal with all Freedom of Information Requests (FOI) which are received in writing within 20 working days, in line with the Freedom of Information Act 2000.

Although requests will be treated along the lines of openness and transparency, some information may be exempt from release.

Quay Primary Healthcare CIC will review all requests and a Public Interest Test will be undertaken before the application of any exemptions for which this applies.

Quay Primary Healthcare CIC publication scheme can be found here: [Insert link to organisational publication scheme]

8. Registration Authority

Smartcards are required to use and access IT systems essential to healthcare provision.

Individuals are granted access to a Smartcard by the organisation's Registration Authority lead. The Registration Authority Lead for Quay Primary Healthcare CIC is Midland and Lancashire Commissioning Support Unit.

The Registration Authority Team verify the identity of all healthcare staff who need to have access to patient identifiable or sensitive data. Individuals are granted access based on their work and their level of involvement in patient care.

The use of Smartcards leaves an audit trail.

Staff should be aware that disciplinary action may be taken if inappropriate action or unauthorised data access has been undertaken or Smartcards are shared.

9. Policy Approval

Quay Primary Healthcare CIC acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders

This Policy has been fully endorsed by the formal approval of Quay Primary Healthcare CIC.

Quay Primary Healthcare CIC will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and contribute to the achievement of the Primary Care objectives and delivery of effective healthcare to the local population

10. Monitoring/Audit

- Quay Primary Healthcare CIC will monitor this Policy through Practice Management Meetings
- An assessment of compliance with requirements within the Data Security and Protection Toolkit will be undertaken each year.

To ensure that the Policy and other relevant Information Governance documents are being followed and implemented, Confidentiality Spot Check Audits will be undertaken throughout the financial year. These audits will identify any areas for improvement which can be provided to the Management team for implementation or risk assessed. Any risks which cannot be mitigated will be noted in the Business Continuity Plan.

11. Information Governance Management

Information Governance Management across the organisation will be co-ordinated By Quay Primary Healthcare CIC Management Team.

The responsibilities to Quay Primary Healthcare CIC Management Team will include, but not be limited to:

- Recommending for approval policies and procedures to be implemented within Quay Primary Healthcare CIC.
- Recommending for approval the annual submission of compliance with requirements in the Data Security and Protection Toolkit and related action plan.
- Co-ordinating and monitoring the Information Governance policy across Quay Primary Healthcare CIC.

Quay Primary Healthcare CIC Management Team will endorse the Information Governance policy for Quay Primary Healthcare CIC.

12. General Provisions

Non-Compliance

Non-compliance with this code of conduct by any person working for Quay Primary Healthcare CIC may result in disciplinary action being taken in accordance with Quay Primary Healthcare CIC 's disciplinary procedure (GPP03), a copy of which can be found on Team Net.

13. Review

This policy will be reviewed on an annual basis or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

Appendix A – Caldicott Principles

The Caldicott Principles revised 2020 are:

Principle 1 - Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 - Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3 - Use the minimum necessary personal confidential data
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes

Principle 5 - Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6 - Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7 - The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Appendix B – Data Protection Act 2018 Principles

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It sits alongside the General Data Protection Regulation (EU) 2016/679 (GDPR), and tailors how the GDPR applies in the UK.

The GDPR sets out the key principles, rights and obligations for most processing of personal data and as a European Regulation, it has direct effect in UK law and automatically applies in the UK.

The Data Protection Act 2018/GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) requires that personal data shall be:
"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency'**);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('**purpose limitation'**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy'**);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation'**);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**')."

Article 5(2) adds that:
“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability’**).”