Document Details	
Title	**IG01 - Policy for handling personal sensitive health information**
Author	CIC Board
Quay Primary Healthcare CIC ref no:	IG01
Version	1.5

Approval process	
Approved by	CIC Board
Date approved	04 December 2015
Lead Director	Medical Director
Category	**Information Governance**
Sub Category	**Information Governance**
Next Review Date	15 Feb 2024
Superseded document (If applicable)	

Distribution	
Who the policy will be distributed to	All Quay Primary Healthcare CIC Team
Method	Email

Version Control		
No:	Date	Amendment
1.1	Feb 2017	Lead Director – details amended
1.2	16 May 2018	Revised in preparation for GDPR
1.3	16 May 2020	Policy review and revision – change of organisation name
1.4	25/11/2021	Change of organisation name – Quay Primary Healthcare CIC
1.5	15/02/2023	Updated ICO certificate expiry date

IG01 - Policy for handling personal sensitive health information

Contents

1. Purpose

To ensure the organisation holds full and concise records for each patient

Clinical staff are required to maintain accurate, useful, and contemporaneous notes for each contact with a patient.

Patient confidentiality is assured.

To comply with the NHS Information Governance requirements.

2. Scope

All staff and workers within the organisation.

3. Policy and Procedure

3.1 Quay Primary Healthcare CIC is compliant with the Data Protection Act (1998) and is registered with the Information Commissioner's Office (ICO). The Corporate Business Manager is responsible for holding proof of registration.

R**egistration Number: ZA108884 exp 21 April 2023**

3.2 Quay Primary Healthcare CIC has registered with the NHS Information Governance Toolkit.

3.3 A Statement of Compliance has been completed for Quay Primary Healthcare CIC and a copy is kept with the Corporate Business Manager.

3.4 Review of Consent Forms and Patient Information Leaflets are carried out regularly.

3.5 All staff with access to records have adequate training for their use and security.

3.6 Staff contracts have appropriate clauses and statements about confidentiality.

3.7 For each patient, essential personal details are recorded, before any clinical intervention. These will include, but not be limited to, the following:

Full name.

Date of Birth.

NHS Number.

Next of Kin.

Address.

Contact telephone numbers.

Record of beliefs – cultural, religious, personal choices – that may affect treatment.

A full Medical History.

3.8 Clinical notes are kept up to date and checked before each clinical intervention.

3.9 Contemporaneous notes are kept concerning all interactions with patients.

3.10 Following patient intervention:

3.10.1 Records of assessing the patient's conditions, taking account of the history (including the symptoms, and psychological and social factors), the patient's views, and where necessary examination of the patient.

3.10.2 Record of advice, investigations, or treatment where necessary.

3.10.3 Record of referring a patient to another practitioner, when this is in the patient's best interests.

Legitimate Relationships – Patient records should only be accessed by those with a legitimate relationship i.e. by the team which is directly involved in that person’s care. The registered GP practice would therefore have access although still limited by the access privileges granted at registration. If a patient was referred by the GP to a hospital or other clinician, a legitimate relationship would be granted to those caring for the patient.

3.10.4 Record of prescribing drugs or treatment, including repeat prescriptions.

3.10.5 Record of any request by a patient for a second opinion.

3.10.6 Clear, accurate and legible records, reporting the relevant clinical findings, the decisions made, the information given to the patient and any drugs prescribed or other investigation or treatment.

3.10.7 Role-Based Access – The elements of a record, which can be accessed, will be dependent on the role of the staff member and this is set up on registration. Most staff will be able to access demographic data using their Smartcard. Clinical information can only be viewed if the job role requires access. Therefore, a receptionist is likely to see minimal information, such as demographic details and the appointment schedule, whereas doctors would be able to see the full record, although these decisions are taken locally.

3.11 All records kept with regard to GMC /NMC publications and guidance.

3.12 All records kept with regard to NHS requirements and guidance. It is the responsibility of the Registered Manager to update this policy bi-annually to check on current guidance.

3.13 Records are kept in a form, and are complete, so that anonymous data can be used in Audits to ensure safety, compliance with Policies and clinical effectiveness.

3.14 There is secure, lockable, storage for all forms of records and data.

3.15 No records are left, or used in a manner, where other patients or visitors can access or read them.

3.16 To protect against loss of data, there is a regular back-up which is either:

External by digital means, NOT a physically portable drive unless encrypted, or Internal to a separate drive kept in a secure and fire-proof place.

3.17 No portable devices are used to hold patient information, including USB sticks, laptop computers or external hard drives, unless encrypted. NHS information is kept in line with the Laptop Security Policy of your local IT Support.

3.18 No Patient information is sent by email except by the protected NHS email service, unless the information is anonymised.

3.19 Patient information is sent by fax to a safe haven fax.

4. The NHS Code of Confidentiality -

4.1 Always log-out of any computer system or application when work on it is finished.

4.2 Do not leave a terminal unattended and logged in.

4.3 Do not share logins with other people. If other staff have need to access records, then appropriate logins will be provided.

4.4 Do not reveal passwords to others.

4.5 Change passwords at regular intervals to prevent anyone else using them.

4.6 Avoid using short passwords, or using names or words that are known to be associated with them (e.g., children's or pets' names or birthdays).

4.7 Always clear the screen of a previous patient's information before seeing another.

4.8 Use a password-protected screensaver to prevent casual viewing of patient information by others.

An audit trail will be kept of every time a Patient NHS Care Record is viewed and edited. Staff should only access patient information when strictly necessary i.e. when they, or their immediate team, are directly involved in the care of that patient. Organisations will run regular comparisons of audit trails with the patients who have attended appointments and Caldicott Guardians will receive automated alerts of irregular activity. Patients will be able to request a copy of their audit trail. NHS Connecting for Health and the BMA have supported the Information Commissioner’s call for tough penalties for those who unlawfully access patient data.

5. Other Relevant Procedural Documents/Publications

https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Confidentiality Policy and Procedure GCP02

6. Equality Impact Assessment

		YES/NO	COMMENTS
1	Does the policy/guidance affect one group less or more favourably than another on the basis of;		
	Race/ethnic origin	No	
	Disability	No	
	Gender	No	
	Religion / belief culture	No	
	Sexual orientation	No	
	Age	No	
2	Is there any evidence that some groups are affected differently ?	No	
3	If you have identified potential discrimination, are any exceptions valid, legal and/ or justifiable?	N/A	
4	Is the impact of the policy/ guidance likely to be negative ?	No	
5	If so can the impact be avoided?	N/A	
6	What alternatives are there to achieving the policy/ guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

7. GDPR

We acknowledge that GDPR is effective from 25th May 2018 and impacts on changes to data protection legislation, however we await the final Data Protection Act 2018 to be released in order that we can attain guidance from the Codes of Practice from the Information Commissioners' Office and the Information Governance Alliance *(part of NHS Digital)*.