Quay Healthcare CI C

Organisation Privacy Notice (v1.2)

Valid From: November 2021

Valid To: November 2023

IDENTITY & CONTACT DETAILS OF THE CONTROLLER AND THE CHIEF PRIVACY OFFER

Quay Healthcare CIC are committed to protecting and respecting your privacy whilst remaining compliant with The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA).

This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Quay Healthcare CIC, are the Data Controller and have an appointed Data Protection Officer, Hayley Gidman, Head of Information Governance, Midlands and Lancashire CSU. Any queries regarding Data Protection issues should be addressed to her at: - Address: Heron House, 120 Grove Road, Fenton, ST4 4LX E mail: mlcsu.dpo@nhs.net / Tel: 01782 872648

PURPOSE OF THE PROCESSING AND THE LEGAL BASIS FOR THE PROCESSING

Quay Healthcare CIC collects and creates personal data for several different purposes:

1. Recruitment and employment.

2. Business development.

3. Provision of services to our members; and

4. Procurement of services

The legal basis for processing personal data for the purpose of recruitment and employment is the pursuit of our legitimate interests of developing our business (recruitment and selection) and subsequently in order to fulfil our legal obligations as an employer and our legitimate interest of striving to provide a safe and rewarding workplace. We will retain personal information we collect in the recruitment and selection process for up to two years following an application for employment which we receive either directly from you or via recruitment agencies. Further information about privacy and data retention is provided in our staff handbook for employees.

The legal basis for processing personal data for the purpose of business development is the pursuit of our legitimate interest in developing our business and undertaking sales and marketing activities.

We acquire personal data from a number of sources including directly from data subjects, from referrals, and from our own research activities such as reviewing websites. We will retain personal information we collect through our processes for as

long as we believe our products and services may be of interest to prospects, members and for members.

Provision of services to our members

The legal basis for processing personal data for the purpose of providing services to our members is either to fulfil our contractual obligations to members or the pursuit of related legitimate interests including maintaining accurate records relating to accounting and finance, monitoring the quality of our services. We will retain personal information we collect through our service delivery processes for as long as such information is relevant to our service delivery model or as defined in our service delivery contract.

Procurement of services

The legal basis for processing personal data for the purpose of procurement is the pursuit of our legitimate interest in maintaining efficient and effective procurement processes. Personal data we collect from suppliers and prospective suppliers is usually supplied directly by data subject or their employer. We will retain personal information we collect through our procurement processes for as long as we need to comply with accounting and taxation rules, policies, and conventions.

Consent

We are required to obtain consent from individuals in order to send them unsolicited electronic marketing messages. We retain evidence of the details of consent which has been provided by our members to process their information in this manner.

LEGITIMATE INTERESTS OF QUAY HEALTHCARE CIC OR THIRD PARTY

Quay Healthcare CIC may use your information for other specific legitimate purposes such as:

- To ensure that content from our site is presented in the most effective manner for you and for your computer.
- To provide you with information, products, or services that you request from us or which we feel may interest you, where you have either explicitly consented to or we believe you have a legitimate interest in.
- To conduct our obligations arising from any contracts entered between you and us.
- To allow you to participate in interactive features of our service when you choose to do so.
- To notify you about changes to our service.

We do not sell, rent, or lease member lists to third parties. However, we may share personal information with companies we feel that there is a genuine possibility of your interest in their services. The lawful basis for this data sharing is the legitimate interest of the third party in developing and growing their business.

INFORMATION WE MAY COLLECT FROM YOU

We may collect and process the following data about you:

Information that you provide by filling in forms on our site or by corresponding with us by phone, email or otherwise. The information you give us may include:

- Name and Company Name
- Email address
- Telephone numbers

If you contact us, we may keep a record of that correspondence.

We may also ask you to complete surveys that we use for research purposes, although you do not have to respond to them.

If you contact us via our Jobs page on our website, we may keep a record of any CV's and Cover Letters sent.

Details of your visits to our website and the resources that you access.

In addition, for users of our service we will need to collect or access details relating to your medical history which may include your medical record. By visiting and using any of our services you are consenting to us using your personal and sensitive personal data in order for us to conduct our services and provide you with medical assistance and consultation. We do this under the following lawful basis to process without consent:

A contract with the individual: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.

A public task: if you need to process personal data to conduct your official functions or a task in the public interest - and you have a legal basis for the processing under UK law - you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.

In addition, as a health service provider and needing to know your medical history and to access your medical records, we also collect and use your sensitive personal data under the following provision:

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member state law or pursuant to contract with a health professional and subject to the conditions and safeguards set out in the regulations.

RECIPIENTS OF THE PERSONAL DATA

Quay Healthcare CIC are required to transfer the personal information provided by its members to third parties in order to fulfil contractual obligations. The following are

categories of recipients that member information or personal data could be transferred to, with your consent or by strict agreement:

- External Service Providers sourced on behalf of our members
- Payment Providers
- Accountancy Services
- Corporate Partners that have referred you to Quay Healthcare CIC
- NHS Trusts/Foundation Trusts
- GP Practices
- NHS Commissioning Support Units
- Integrated Care Boards
- NHS England (NHSE) and NHS Digital (NHSD)
- Local Authorities
- Other ‘data processors’ which you will be informed of

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required. We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All information you provide to us is stored on our secure servers. However, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. We will not disclose your information to any of the relevant third parti es listed above for marketing purposes.

Our Data Protection Officer can provide you with contact details of our third parties upon request if required.

NATIONAL OPT-OUT FACILITY

You can choose whether your confidential patient information is used for research and planning. It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

Making your data opt-out choice:

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people’s health. You can also still consent to take part in a specific research project.

Will choosing this opt- out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used. If you do not want your confidential patient information to be used for research and planning, you can choose to opt out securely online or through a telephone service. You can change your choice at any time. To find out more or to make your choice visit www.nhs.uk/your-nhs-data-matters or call 0300 303 5678.

DETAILS OF TRANSFERS TO THIRD COUNTRIES & SAFEGUARDS

Quay Healthcare CIC do not store personal data on information systems that require transfer to third party countries. We ensure that all other personally identifiable information held on our members and employees remains within the EEA.

RETENTION PERIOD

We retain all member information for 5 years after they last interacted with us unless:

a) you ask us to remove it

b) we believe that you are no longer interested in our business

c) we no longer need it for the purposes it was collected.

Where there has been a peri od of 5 years and there has been no interaction between the organisation and the member, their information is erased and securely disposed of.

RIGHTS OF DATA SUBJECTS

As a Data Subject (individual) which Quay Healthcare CIC process information on behalf of, you have the right to request access to, and the rectification or erasure of personal data that we hold about you as well as a right to object to and to a restriction of our processing of your personal data at any given time.

You can do this by contacting our Data Protection Officer through the contact details provided on page 1 of this policy. You also have a right to lodge a complaint with the Supervisory Authority (Information Commissioners Office (ICO) in the UK - at www.ico.org.uk), should you feel that we have not managed your information in line with legislative and regulatory requirements.

You have the right to make a Data Subject Access Request to Quay Healthcare CIC, Data Protection Officer if you wish to determine what information we hold on you. We welcome these requests and aim to respond within the timeframes set out in the GDPR.

AUTOMATED DECISION MAKING, INCLUDING PROFILING & INFORMATION ABOUT HOW DECISIONS ARE MADE, THE SIGNIFICANCE OF THE CONSEQUECES.

IP Addresses

We may collect information about your computer, including where available your IP address, geographic location (if you allow when prompted by your browser), operating system and browser type, for system administration when you access our website. We use this information for statistical

data about our users' browsing actions and patterns when they access our website.

Changing your Privacy Settings or Unsubscribing from our Privacy Policy

In the event that you wish to you alter your Privacy settings or opt-out, you are able to do this by emailing our Data Protection Officer. Our Data Protection Officer shall provide you with contact details of our third parties upon request if required.

Marketing Communications

We may send out email communication such as our newsletter to keep you up to date with all the latest News, projects, and service updates from us. If you wish to unsubscribe from these emails, you can do so at any time by contacting Emma Glover, administrator at Quay Healthcare CI C at emma.glover@nhs.net. Please note that even if you decide not to subscribe to, or to unsubscribe, from promotional email messages, we may still need to contact you with important member information. For example, even if you have unsubscribed from our promotional email messages, we will still send you confirmations when you confirm services from us.

Changes to our Privacy Policy

We may change this Privacy Policy from time to time. If we make significant changes in the way we treat your personal information, or to the Privacy Policy, we will make that clear on our websites or by email, so that you are able to review the changes.

CONTACT

Questions, comments, and requests regarding this privacy policy are welcomed and should either be emailed to our Data Protection Officer (see page 1) or Amy Cannon, Business Operations Manager at amy.cannon@nhs.net

QUAY HEALTHCARE CIC PRIVACY NOTICE FOR PATIENTS

What is a Privacy Notice?

A Privacy Notice (or 'Fair Processing Notice') is an explanation of what information the Practice collects on patients, and how it is used. Being transparent and providing clear information to patients about how an organisation uses their personal data is an essential requirement of the Data Protection Act 1998.

Under the DPA, the first principle is to process personal data in a fair and lawful manner, and applies to everything that is done with patient's personal information. In practice, this means that the Practice must;

- have legitimate reasons for the use or collection of personal data
- not use the data in a way that may cause adverse effects on the individuals (e.g. improper sharing of their information with 3rd parties)
- be transparent about how you the data will be used, and give appropriate privacy notices when collecting their personal data
- handle personal data only as reasonably expected to do so
- make no unlawful use of the collected data

Fair Processing

Personal data must be processed in a fair manner – the DPA says that information should be treated as being obtained fairly if it is provided by a person who is legally authorised or required to provide it. Fair Processing means that the Practice has to be clear and open with people about how their information is used.

Providing a 'Privacy Notice' is a way of stating the Organisation's commitment to being transparent and is a part of fair processing, however you also need to consider the effects of processing on the individuals and patients concerned;

- What information are we collecting?
- Who collects the data?
- How is it collected?
- Why do we collect it?
- How will we use the data?
- Who will we share it with?
- What is the effect on the individuals?
- If we use it as intended, will it cause individuals to object or comply

Data Controllers

Under the Data Protection Act, the data controller is the person or organisation that will decide the purpose and the manner in which any personal data will be processed – they have overall control of the data they collect and decide how and why it will be processed.

A GP Practice is a data controller for the patient information it collects, and should already have data processing arrangements with third parties (e.g. IT systems providers) to ensure they do not use or access data unlawfully; the data controllers will have ultimate responsibility for the Practices' compliance with the DPA.

Risk Stratification

This is a process to identify and manage patients that are more likely to need secondary care – information is collected in order to assess their 'Risk Score' and is sent to NHS organisations to assess and return the results to the GP Practice. This is an acceptable way of assessing patients' needs and prevent ill health, however it is also regarded as a disclosure of personal information, and patients have the option to opt out of any data collection at the Practice, and needs to be made clear to them.

Invoice Validations

If a patient has had NHS treatment, their personal information may be shared within a secure and confidential environment to determine which ICB should pay for the treatment received. This means sharing identifiable information such as name, address, date of treatment etc. to enable the billing process.

Partner Organisations

If the Practice shares information with any external organisations (within or outside the NHS), then let patients know by listing them. Partner organisations will usually include NHS organisations (hospitals, ICBs, NHS England etc.) other public sectors (Education, Police, Fire etc.) and any other Data Processors that may be carrying out specific project work with the Practice (e.g. Diabetes UK).

Access to Personal Information

The DPA gives patients the right to view any information held about them – the 'Right of Subject Access'. Explain the process and who to contact. You can find your practice registration number by entering your Practice name in the 'Name' box here; ico.org.uk/ESDWebPages/Search

How we use your information

This privacy notice explains why we as an organisation collect information about our patients and how we use that information.

Quay Healthcare CIC manages patient information in accordance with existing laws and with guidance from organisations that govern the provision of healthcare in England such as the **Department of Health** and the General Medical Council.

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 1998
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality and Information Security

As data controllers, we have fair processing responsibilities under the **Data Protection Act 1998**. In practice, this means ensuring that your personal confidential data (PCD) is handled clearly and transparently, and in a reasonably expected way.

The **Health and Social Care Act 2012** changed the way that personal confidential data is processed, therefore it is important that our patients are aware of and understand these changes, and that you have an opportunity to object and know how to do so.

The health care professionals who provide you with care maintain records about your health and any NHS treatment or care you have received (e.g. NHS Hospital Trust, GP Surgery, Walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

NHS health records may be processed electronically, on paper or a mixture of both; a combination of working practices and technology are used to ensure that your information is kept confidential and secure. Records held by this Organisation may include the following information:

- Details about you, such as address and next of kin
- Any contact the organisation has had with you, including appointments (emergency or scheduled), clinic visits, etc.
- Notes and reports about your health
- Details about treatment and care received
- Results of investigations, such as laboratory tests, x-rays, etc.
- Relevant information from other health professionals, relatives or those who care for you

The organisation collects and holds data for the sole purpose of providing healthcare services to our patients and we will ensure that the information is kept confidential. However, we can disclose personal information if:

It is required by law

1. You provide consent – either implicitly or for the sake of their own care, or explicitly for other purposes

2. It is justified to be in the public interest

Some of this information will be held centrally and used for statistical purposes. Where we hold data centrally, we take strict and secure measures to ensure that individual patients cannot be identified.

Information may be used for **clinical audit** purposes to monitor the quality of service provided and may be held centrally and used for statistical purposes. Where we do this, we ensure that patient records cannot be identified.

Sometimes your information may be requested to be used for **clinical research** purposes – the organisation will always endeavour to gain your consent before releasing the information.

Improvements in information technology are also making it possible for us to share data with other healthcare providers with the objective of providing you with better care.

Patients can choose to withdraw their consent to their data being used in this way. When the organisation is about to participate in any new data-sharing scheme we will make patients aware by displaying prominent notices on our website at least four weeks before the scheme is due to start. We will also explain clearly what you have to do to 'opt-out' of each new scheme.

A patient can object to their personal information being shared with other health care providers but if this limits the treatment that you can receive then the doctor will explain this to you at the time.

Telephones

If you provide us with your mobile phone number, we may use this to send you reminders about any appointments or other health screening information being carried out.

Quay Healthcare has the ability to record telephone calls to protect patients and staff and other health workers. Patients are protected by the ability to record our conversations with you, staff and other health workers are protected from potential abuse. Calls to and from Quay staff are all recorded. We also occasionally use recordings for staff training and quality control.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations:

- NHS Trusts
- GP Practices
- Specialist Trusts
- Community Trusts
- Independent Contractors such as dentists, opticians, pharmacists

- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Integrated Care Boards
- Social Care Services
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police
- Other 'data processors'

Access to personal information

You have a right under the **Data Protection Act 1998** to access/view information the organisation holds about you, and to have it amended or removed should it be inaccurate. This is known as 'the right of subject access'. If we do hold information about you we will:

- give you a description of it
- tell you why we are holding it
- tell you who it could be disclosed to
- let you have a copy of the information in an intelligible form

If you would like to make a 'subject access request', please contact the practice manager in writing. There may be a charge for this service. Any changes to this notice will be published on our website and on the practice notice board.

The practice is registered as a data controller under the Data Protection Act 1998. The registration number is **ZA108884** and can be viewed online in the public register at ico.org.uk

Change of Details

It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

Notification

The Data Protection Act 1998 requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information. This information is publicly available on the Information

Commissioners Office website www.ico.org.uk. The practice is registered with the Information Commissioners Office (ICO).

Who is the Data Controller?

The Data Controller, responsible for keeping your information secure and confidential is Lorraine Stratulis – Chief Operating Officer. Any changes to this notice will be published on our website and displayed in prominent notices on our website.

The Partnership is registered as a data controller under the Data Protection Act 1998 **ZA108884**. Our registration can be viewed on-line in the public register at www.ico.org.uk

Data Protection Officer

Craig Walker – Head of Information Governance and Quality Assurance
St Helens & Knowsley Teaching Hospitals NHS Trust
Alexandra Business Park
Court Building
PRESCOTT Road
St Helens
WA10 3TP

Further information

Further information about the way in which the NHS uses personal information and your rights in that respect can be found in:

- The NHS Care Record Guarantee: www.nigb.nhs.uk/pubs/nhscrg.pdf
- The NHS Constitution: www.gov.uk/government/publications/the-nhs-constitution-for-england
- NHS Digital's Guide to Confidentiality in Health & Social Care gives more information on the rules around information sharing: content.digital.nhs.uk/article/4979/Assuring-information

An independent review of information about patients is shared across the health and care system led by Dame Fiona Caldicott was conducted in 2012. The report, Information: To share or not to share? The Information Governance Review, be found at: www.gov.uk/government/publications/the-information-governance-review

NHS England – Better Data, Informed Commissioning, Driving Improved Outcomes: Clinical Data Sets provides further information about the data flowing within the NHS to support commissioning.

Please visit the NHS Digital website for further information about their work. Information about their responsibility for collecting data from across the health and social care system can be found.

The Information Commissioner's Office is the Regulator for the Data Protection Act 1998 and offer independent advice and guidance on the law and personal data,

including your rights and how to access your personal information. For further information please visit the www.ico.org.uk