

# Privacy Notice

**Hartlepool & East Durham Mind**

**Crown Buildings**

**Tees Street**

**Hartlepool**

**TS24 8HB**

**Tel: 01429 269303**

**Fax: 01429 422262**

**Email: [information@hartlepoolmind.co.uk](mailto:information@hartlepoolmind.co.uk)**

**Performance & Governance Manager (Information Governance): Jill Best**

In order to provide a suitable and quality service to you, we need to collect and process different types of information about you.

## Types of information

- **Personal Confidential Information** – this term describes personal information or data about identified or identifiable individuals, which should be kept private or secret. For the purposes of this notice 'personal' includes the Data Protection Act and General Data Protection Regulations definition of personal data, but it is adapted to include deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive', as defined in the Data Protection Act and General Data Protection Regulations.
- **Pseudonymised** – this is data that has undergone a technical process that replaces your identifiable information such as NHS number, postcode, date of birth with a unique identifier, which obscures the 'real world' identity of the individual patient to those working with the data
- **Anonymised** – this is data about individuals but with identifying details removed so that there is little or no risk of the individual being re-identified
- **Aggregated** – Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data such as age ranges.

## Why do we collect this information?

**Personal** information is collected to ensure we are able to contact you when required and to confirm we are providing the right care to the right person. **Confidential** information is collected to keep a record of the care we provide to you and to confirm you are receiving the most appropriate support to help you with the difficulties we are experiencing.

Information is given to commissioners of the service and is **aggregated** before it is sent to them. We have a duty to share this information to evidence that we are providing care within the requirements of our contract with them and the law and that we are meeting expected performance targets. No identifiable information is shared with commissioners. Information uploaded to NHS Digital is **pseudonymised and aggregated** by NHS Digital. Detail on the content of your appointments is not shared, only attendance at appointments, scores on clinical outcome measures and demographic information such as age and gender is given. NHS digital

will not share any personal identifiable information without explicit consent. Further information can be found at

<https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/how-we-look-after-your-health-and-care-information>

### **Can I see the information you have about me?**

Yes, you are entitled to view and have a copy of all the information we have recorded about you. To access this information, you need to request it in writing to the address above. We will respond to your request within one month of receiving it.

### **Do you share this information with anyone else?**

**Personal and confidential** information will not be shared with anyone other than those mentioned above without your consent unless we have concerns about any of the following:

- Pose a risk to the public or Staff
- Terrorism (The Prevention of Terrorism Act)
- Committing a crime
- Serious physical harm to others
- Abuse of a child
- Serious harm to yourself

In these circumstances we have an obligation to share our concerns to keep you and other people safe. The nature of the concern will depend on who we share the information with. This includes, but is not limited to, the police, your GP, social services or the crisis team. Although we do not require your consent in these circumstances, we will always discuss it with you and explain our concerns and the reason we feel the information needs to be shared.

### **Do you have a legal basis to process this information about me?**

Under the law we need to make sure that any information processing we do is fair, lawful and transparent. Within the General Data Protection Regulations (2018) we must ensure that we meet an Article 6 condition and an Article 9 condition. We also have to comply with the Common Law Duty of Confidentiality which ensures your information is protected and remains confidential. This means that where a legal basis for using your personal or confidential information does not exist, we will not do so.

Purpose / use of data	Example	GDPR Lawful Processing Requirements		
		Article 6	Article 9	Common law duty of confidentiality
Individual care	Referrals, recording of appointments / clinical notes	6(1)(e) or (c)	9(2)(h)	Implied & explicit consent
Secondary uses – flows to NHS Digital & commissioners of services	Collection of mental health services data set	6(1)(c)	9(2)(h) or (i)	Directions (opt out can be considered in some circumstances). Detail of appointments are not shared.
Secondary uses – planning and running NHS (other mandatory flow)	CQC powers to require information and records	6(1)(e) for CQC 6(1)(c) for the provider	9(2)(h) or (i)	Legally required
Secondary uses – planning and running NHS (S251 – Reg 5)	National Clinical audits	6(1)(e)	9(2)(h) or (i)	S251
Secondary uses – research (consented)	Research on specific areas of care (consent will be asked prior to the sharing of any information)	6(1)(e)	9(2)(j)	Explicit consent

Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject

Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 9(2)(h) 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 referred to in paragraph 3;

Article 9(2)(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

NHS Digital is developing a new system to support the national data opt-out which will give patients more control over how their personally identifiable data is used. The system will let patients exercise their right to make an informed choice about whether their personally identifiable data is only used for their individual care and treatment or also shared for research and planning purposes. Further information regarding opting out is available from the NHS Digital website or your GP.

### **How do you keep my information safe?**

All staff working or volunteering for the organisation have a legal duty to keep information about you strictly confidential.

We store your information on an information management system called IAPTus, which is provided by Mayden. Their system security is of the same standard used by the Ministry of Defence and the NHS. Each member of staff has a username and password for the system. There is a security process that needs to be completed before the staff member can get access to the system. Access to records is monitored and restricted to those staff members who have a legitimate purpose for accessing it. This includes the administration team, data team, management team and allocated clinician. All access to records must be justified. The business intelligence team monitor access and report on this to the Performance and Governance Manager on a regular basis.

We also store minimal paper records which are used as a backup if the electronic system is not accessible. These are stored in a locked filing cabinet whilst you are using the service. The filing cabinet is in a locked room with a keypad lock; the code for which is changed monthly. We have a secure storage unit which is accessible by key personnel within the organisation only. The organisation performs regular audits of its security processes to ensure the highest level of security is maintained.

We are required to retain copies of your records for 20 years.

### **Can I object to my information being processed?**

The organisation is obliged by law to keep a record of services that we have provided to you in a similar way that your doctor needs to keep a record of any appointments they have with you. You do have a right to object to this information being processed other than for your individual care.

If you wish to discuss the right to object further, or to speak to somebody to understand what impact this may have, if any, please contact us using the contact details at the top of this document.

## **How can I complain if I am not happy with how my information is processed?**

If you are not happy with how your information is processed you can raise your concerns by contacting us on the details at the top of this page.