DATA PROTECTION IMPACT ASSESSMENT FOR COLLECTION OF HEALTH DATA FOR

ARBOR NEUROREHABILITAION SERVICES LTD

Who is completing this DPIA?

SUBMITTING CONTROLLER DETAILS
Name of Controller
Arbor Neurorehabilitation Services Limited
Title of Data Protection Officer
Dr Kesta Purt and Mrs Sarah Gibbin
Contact Details
0117 287 2088 info@arbor-neuro.com

Section 1 – Identifying the Need for a DPIA

This section outlines the reasons a DPIA has been identified as necessary.

THE NEED FOR A DPIA
1. Explain what the project/purpose case you are working on hopes to achieve.
The purpose of collecting health data is to provide neurorehabilitation therapy services including clinical psychology, neuropsychology, speech and language therapy, physiotherapy, occupational therapy, dementia nursing, family therapy and therapy assistant services to support individuals with their neuro rehabilitation.
2. Outline what type of data processing this case involves.
This case involves the collection, analysis, and storage of sensitive health data, including personal and clinical health information about individuals undergoing therapy or assessments.
3. Summarise why You think it's necessary to complete a Data Protection Impact Assessment for this case.
A DPIA is necessary because the processing involves sensitive health data, which could impact the privacy and rights of individuals if not managed properly. The assessments and therapy involve high-risk data processing activities under UK data protection laws.

Section 2 – Describe the processing activities

This section outlines the processing activities, the context of the processing, and the purpose of the processing.

THE NATURE OF THE PROCESSING
4. Explain your process for collecting, using, storing, and deleting the data?
Data is collected through initial consultations, neurorehabilitation sessions, therapy sessions, and assessment interviews. It is stored securely in electronic health records and physical files, with regular reviews to ensure data accuracy and relevance. Data deletion protocols are in place for data no longer needed.
5. Where will you source this data from?
Data is sourced directly from clients during therapy sessions and assessments, as well as from any referring case managers or healthcare providers, with the client's consent.
6. List any individuals/entities you will share this data with.
Data may be shared with case managers, litigation lawyers, deputyships or other healthcare professionals involved in the client's care, such as therapists or GPs, with explicit consent from the client.
7. What, if any, of your data processing activities can be labelled as high risk? *High risk data processing means processing that results in a high risk to the rights and freedoms of individuals e.g., health data processing.*
The processing of health data for therapy and assessments is considered high-risk due to the sensitivity of the information and the potential impact on individual rights and freedoms.

THE SCOPE OF THE PROCESSING
1. What type of data is this, and does it involve personal information that is considered special category data?
The data involves personal information, including special category data such as health records, neurodevelopmental and psychological evaluations, speech and language observations, physiotherapy notes and occupational therapy notes.
2. Outline how much data you will be collecting and using.
Data is collected on an ongoing basis as needed for therapy and assessments. It is retained in accordance with professional guidelines, typically for at least seven years following the end of treatment, or until the child's 25th birthday. Neuropsychological test data is held for 20 years.
3. How often will you collect this data, and how long do you plan to retain this data?
See above.
4. How many individuals are affected by your processing of this data?
The processing affects adults and adolescents, seeking therapy support and services.
5. What geographical area does this data cover?
The data primarily covers individuals within the UK.

THE CONTEXT OF THE PROCESSING

1. Describe the nature of your relationship with the individual in question.

The relationship is a professional therapeutic one, where clients expect confidentiality and professional handling of their data.

2. How much control does this individual have over their data processing, and do they expect you to use their data this way?

Clients have control over their data to the extent of granting consent for its use and can request access or corrections to their records.

In cases where clients lack the mental capacity to consent to treatment or understand the implications of data processing, we adhere to the guidelines set out under the Mental Capacity Act 2005. We ensure that any processing of personal data is done in the best interests of the client, and decisions are made through consultation with their appointed deputies or legal representatives. Careful documentation of all decisions and consultations is maintained to uphold transparency and accountability.

3. Is the individual in question a child, or classed as vulnerable?
Some examples of vulnerable groups include individuals with disabilities, the elderly, and individuals who are in a position of dependence. For more information, refer to the following ICO Guidelines here

Some individuals may be considered vulnerable, such as children or those with mental health conditions, including those with neurodevelopmental conditions.

4. Are there any known issues or risks associated with this type of data processing? Is it a new or different type of processing?

No known risks.

5. What is the current state of technology in this field for the processing? Are there any issues with this approach that are classed as public concern, which need to be factored in?
For example, what case management software do you utilise in your practice to process data, if any, and are there any concerns regarding this.

We use safe, secure and GDPR compliant client management/email systems – all in line with usual neurorehabilitation therapy industry standards.

6. Are you signed up to any approved code of conduct or certification scheme in regard to your processing? If so, please detail this below.

We abide by the codes of conduct of our regulators, including the Health & Care Professions Council (HCPC); the British Psychological Society (BPS); the Royal College of Speech and Language Therapists, the Royal College of Occupational Therapy, the Chartered Society of Physiotherapy, the Royal College of Nursing, UK Council for Psychotherapy, Association for Family Therapy and Systemic Practice, Nursing and Midwifery Council, as applicable.

THE PURPOSE OF THE PROCESSING

1. What do you hope to gain from processing this personal data?

The processing aims to provide effective therapeutic interventions and therapy services to improve clients' neurorehabilitation outcomes.

2. What is your intended effect on the individuals? How do you hope this processing will assist with that?
The processing is intended to positively impact individuals by providing tailored therapeutic support and accurate assessments to address their specific needs.
3. Outline the benefits of processing for a) you and b) more broadly. *For example, the benefits for processing may include helping your patient, and the broader benefit includes aggregating the data to understand what treatment works well, to replicate on others.*
Benefits include enhanced neurorehabilitation outcomes and overall well-being for clients, as well as contributing to broader research and understanding of effective neurorehabilitation therapies and techniques.

Section 3 – The Consultation

This section outlines if, and how, any consultations will occur with others regarding the data processing.

THE PURPOSE OF THE PROCESSING
1. Describe when, and how, you will speak to others for their views on the data processing. *For example, other healthcare professionals, researchers, regulatory bodies, etc.*
Consultations may occur with other healthcare professionals involved in the client's care.
2. If it is not appropriate to seek others' views, please outline why this is.
n/a
3. Who else at your practice will be involved in the data processing?
Other clinicians and administrative staff involved in the practice may assist with data processing, following strict data protection protocols. We have proper agreements with data processing/data sharing clauses in place.
4. Do you require your data processors to assist with the processing?
Yes – see above with respect to the clauses we have included in our contracts with them.
5. Will you speak with security experts, or any other experts, in relation to the processing?
No.

Section 4 – The Necessity and Proportionality of the Processing

This section outlines why the processing is both necessary and proportionate for the purposes of the processing.

THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING
1. What is your lawful basis for the processing? Review the below options and select all that apply.
☒ **Consent** – the individual has provided consent for us to process their data for these specific purposes. ☒ **Contract** – the processing is needed to carry out a contract held with the individual e.g., to provide healthcare services to them. ☐ **Legal Obligation** – the processing is required to comply with the law ☐ **Vital –** the processing is needed to protect someone's life ☐ **Public Task** – the processing is required for us to perform a task in the public interest. ☒ **Legitimate Interests** – this processing is necessary for our legitimate interests, or that of a third party.
2. Does your processing achieve your purpose?
The processing is based on explicit consent from individuals for health-related data, and it may also be necessary for the performance of a contract (therapy provision) and for legitimate interests of providing healthcare services.
3. Is there another way that could achieve the same outcome?
No.
4. How will you avoid and prevent your service expanding, and as a result processing, from the original scope over time (also known as 'function creep')?
Regular audits and reviews will be conducted to ensure data processing remains within the original scope and purpose.
5. Outline how you plan to ensure that the data collected is kept accurately, and the collection and processing is kept to a minimum?
Data accuracy is maintained through regular reviews, and only data necessary for the specific therapeutic or assessment purposes is collected.
6. What information about your processing will you give to the individual(s) in question?
Clients are informed about their data rights, including access, rectification, and erasure options, and have a clear complaints process.
7. How will you help to support the individua's rights in terms of data processing?
By providing details about their rights in our privacy policy (which is available on our website) and signposting this in our Terms and Conditions.
8. Outline the measures You take to ensure your data processors comply with your processes to protect individual rights during the processing.
We have robust data processing and data sharing clauses in our agreements with associates, virtual assistants and other third party suppliers.
9. Outline your process used to safeguard any international transfers of the data.

International transfers of data can include storing data on software such as Dropbox and Google Drive because their servers are based in the US.
Any international data transfers, such as using cloud-based storage services, will be safeguarded by ensuring compliance with UK GDPR standards and using approved mechanisms like Standard Contractual Clauses.

Section 5 – Identifying, Assessing and Reducing the Risks to Processing

This section flags any risks associated with the processing, and identifies the likelihood of harm occurring.

THE RISKS OF THE PROCESSING
1. Describe a risk associated with the processing, and the potential impact this risk materialising could have on the individual(s).
A potential risk is unauthorised access to sensitive health data, which could lead to privacy breaches and distress for individuals.
2. How likely is it that this harm will occur?
☒ Remote ☐ Possible ☐ Probable
3. How severe would this harm be?
☐ Minimal ☒ Significant ☐ Severe
4. What is the overall risk?
☒ Low ☐ Medium ☐ High
5. How could you reduce or eliminate this risk?
Implementing strong encryption, access controls, staff training on data protection, and regular security audits to reduce risk.
6. What effect does your solution have on this risk?
☐ Eliminated ☒ Reduced ☐ Accepted
7. What proportion, if any, of elements of the risk remain?

☐ Eliminated ☒ Reduced ☐ Accepted
8. Do you approve of this measure to reduce the risk?
Yes

Section 6 – Outcome

Step	Responsible Person and Notes	Guidance Notes
Actions Approved By	Dr Kesta Purt and Mrs Sarah Gibbin	*The practice manager and data protection officer will oversee compliance with this DPIA, ensuring all staff are aware of data protection responsibilities.*
Remaining Risks Approved By	Dr Kesta Purt and Mrs Sarah Gibbin	*Contact the ICO before moving ahead if there are any unresolved high risks.*
DPO's Advice Summary	The DPO advised the following: The DPO will provide guidance on implementing best practices for data protection and ensuring compliance with legal obligations. Regular reviews will be scheduled to ensure ongoing compliance.	*Detail the DPO's suggestions on safety measures and moving forward.*
Is DPO's Advice Followed?	Yes	*If not, explain why here.*
Consultation Responses Reviewed By	Dr Kesta Purt and Mrs Sarah Gibbin	*Explain any changes that differ from public or individual feedback.*
Future Review Date	10th June 2026	*Ensure DPO is set to review ongoing compliance on [Date].*