**Data Sharing Agreement – Controller to Processor**

**Guidance Notes**

For organisations with whom you share personal information, but which are processors not controllers, it is a legal obligation to have a Data Sharing Agreement in place.

**Controller to Processor Data Sharing Agreement**

**BETWEEN**

**The Healthcare Business**

***[insert name]***

**(the Data Controller)**

**AND**

**The Provider**

***[insert name]***

**(the Data Processor)**

**In support of *[insert name of contract here]***

**This agreement** is made on **dd/mm/yyyy**

**1. Background Information**

* 1. [Insert healthcare business name] and [the name of the Provider] have entered into a contract, which includes processing personal data for the purposes specified in Schedule 1 of this document.
	2. For the purposes of this agreement and in compliance with the provisions of the UK GDPR, **[name of the Provider]** is the Data Processor who is processing personal data on behalf of **[insert healthcare business name]** who is the Data Controller and legally responsible for that data processing under the UK GDPR.
	3. The UK General Data Protection Regulation (amongst other things) requires a data controller, when using the services of another organisation or company to process personal data on their behalf (a data processor), to:
	4. choose a data processor who can provide sufficient guarantees about their data security measures to protect the personal data they will be processing as part of the contract;
	5. take reasonable steps to make sure those security measures are in place and sustained; and
	6. document what the data processor is allowed to do with the personal data in a written contract. The contract must include:
		1. what they can and what they cannot do with the personal data;
		2. what security measures must be in place to protect the data (they must be equivalent to the level of security imposed on the data controller by the Act);
		3. what procedures must be followed if there is a security breach (incident); and
		4. any other arrangements, i.e. sub-contracting, termination of contract etc., that need to be included to secure and control the data.
	7. This contract neither overrides nor replaces any main service contract, but instead is supplementary to it. It is issued in accordance with the UK GDPR Principle, which requires [insert healthcare business NAME] as the Data Controller to set out the terms and conditions for the provision of the services provided by [name of Provider] as the Data Processor.
	8. There is a requirement upon the Data Processor to only process data as instructed by the Data Controller. [Insert healthcare business NAME] as the Data Controller remains legally responsible for the personal data even when it is processed by [the Provider’s name] as the Data Processor. [Insert NAME]must take steps to ensure the personal data remains protected, the liabilities and risks are appropriately managed, data is processed lawfully, and the contract is legally enforceable.

**2. Data Controller Responsibilities**

2.1 [Insert healthcare business NAME] is the Data Controller of the personal data and is responsible for ensuring it is processed fairly and lawfully and in accordance with the UK General Data Protection Regulation.

2.2 Under the UK GDPR, it is the legal duty of the Data Controller to ensure the data protection principles are met when personal data that s/he is a data controller for is used (unless an exemption applies).

2.3 The Data Controller remains legally responsible for the data processing carried out by the contracted Data Processor.

2.4 The Data Controller shall not instruct the Data Processor to process personal data on his/her behalf under this contract where the Data Controller him/herself does not have a secure basis in law to process that data.

2.5 The Principles are set out in the UK GDPR. The 6th Principle requires that, where processing of personal data is carried out by a data processor on behalf of the Data Controller, the Data Controller must:

* 1. choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
	2. take reasonable steps to ensure compliance with those measures.

Where processing of personal data is carried out by a data processor on behalf of the Data Controller, the Data Controller is not to be regarded as complying with the 6th Principle unless:

* 1. the processing is carried out under contract
		1. which is made or evidenced in writing, and
		2. under which the Data Processor is to act only on instructions from the Data Controller, and
	2. the contract requires the Data Processor to comply with obligations equivalent to those imposed on the Data Controller by the 6th Principle.

2.6 [Insert healthcare business NAME], as the Data Controller, is entitled during the term of this contract, to require the Provider, as the Data Processor, to provide reasonable assurance that the technical and organisational security measures adequately protect the personal data it is contracted to process. This includes the Data Controller’s entitlement to audit the Data Processor’s premises, systems, procedures, documents, data protection training records and staff as may be desirable or necessary to ensure compliance with this contract, the service contract and/or with the law.

**3. Data Processor Responsibilities**

* 1. [The name of the Provider] is the Data Processor and shall at all times process personal data only as instructed to do so by **[**Insert healthcare business NAME**]** as the Data Controller and in accordance with the General Data Protection Regulation and this contract.
	2. The Provider, as the Data Processor, shall have in place appropriate technical and organisational security measures that protect the personal data it is contracted to process on behalf of the Data Controller from unauthorised or unlawful processing, accidental loss, destruction or damage.
	3. The Provider shall provide reasonable assurances and guarantees to the Data Controller (as required) that those technical and organisational security measures in place are both appropriate and effective in protecting the processing of personal data.
	4. The Provider agrees to maintain good information governance standards and practices.
	5. The Data Processor shall not share the personal data with any third party without the prior written permission of the Data Controller or process personal data in any way or for any purpose that has not been instructed and authorised by the Data Controller.
	6. Neither shall the Provider sub-contract a third party to process the Data Controller’s personal data without the prior knowledge and written agreement of the Data Controller, and only then having provided all the necessary assurance and guarantees of their adequate organisational and technical security measures.
	7. The Data Processor shall not transfer or permit the transfer of the personal data on to any territory outside the UK without the prior knowledge and written agreement of the Data Controller.

**4. Data Security Requirements**

The Data Processor shall:

* 1. Have regard to the state of technological development and to the cost of implementing any measures, provide a level of security (including appropriate technical and organisational measures) appropriate to the harm that might result from unauthorised or unlawful processing of personal data or the accidental loss, damage or destruction of personal data and the nature of that personal data.
	2. Ensure that access to the personal data is limited to those employees who need access to meet the Data Processor’s obligations under this contract.
	3. Take reasonable steps to ensure the reliability of their personnel who have access to the personal data, which shall include ensuring that all staff engaged by the Provider understand the confidential nature of the personal data; and
		1. have received appropriate training annually in data protection prior to their use of the data, and
		2. have signed a written undertaking that they understand and will act in accordance with their responsibilities for confidentiality under contract.

The Data Processor shall ensure:

* 1. That it has properly configured access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control.
	2. That suitable and effective authentication processes are established and used to protect personal data.
	3. That the personal data is backed up on a regular basis and that any backup data is subject to vigorous security measures as necessary to protect the availability, integrity and confidentiality of the data.
	4. That robust and tested business continuity measures are in place to protect the confidentiality, integrity and availability of the Data Controller’s personal data.
	5. Data transferred electronically is encrypted in accordance with national standards.
	6. Employees are not able to access the data remotely, e.g. from home or via their own electronic device or internet portal, other than through a secure electronic network and in accordance with organisational remote working policy. No data shall be stored in such devices.
	7. Data that requires disposal is disposed of securely and confidentially in accordance with the secure destruction requirements specified in section 8.

**5. Serious Information Breach Incident, Incident Reporting and Duty of Candour**

* 1. The Data Processor shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of personal data.
	2. The Data Processor shall immediately report any information security incident related to the personal data subject to this contract to the Data Controller and undertakes to also fully cooperate with the Data Controller’s incident investigation requirements.
	3. In so far as the Data Controller is responsible for the personal data, it is the Data Controller’s responsibility to ensure that the incident is reported in accordance with the law, informing the relevant data subjects as appropriate.

5.4 The Data Processor will have processes in place for the identification and management of a subject access request received in relation to the Data Controller’s data subjects.

5.5 The Data Processor shall immediately report any subject access request related to the personal data subject to this contract to the Data Controller and undertakes to also fully cooperate with the Data Controller’s investigation including a provision of all relevant personal data which is the subject of the request to the Data Controller within [insert timeframe].

**6. Process for Agreeing Variations**

* 1. Any variation to the terms of this contract shall be agreed in writing by the Parties and in accordance with the contract management conditions set out in the main contract.

**7. Dispute Resolution Process**

* 1. Both Parties shall aim to resolve all disputes, differences and questions by means of cooperation and consultation and in accordance with the dispute resolution process specified in the main contract.

**8. Secure Destruction**

* 1. The Data Processor shall ensure that personal data held in paper form (regardless of whether originally provided by the Data Controller or printed from the Data Processor’s IT systems) is destroyed using a cross-cut shredder or subcontracted to a confidential waste company.
	2. The Data Processor shall ensure that electronic storage media used to hold, or process personal data is destroyed or overwritten.
	3. In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.
	4. The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of personal data at the conclusion of the contract.

**9. Exit From Contract**

* 1. The Data Controller may terminate this contract with immediate effect by written notice to the Data Processor on or at any time after the occurrence of an event that gives rise to an information security incident, or otherwise poses a risk of non-compliance with the Data Protection Principles.
	2. In order to protect the personal data, the Data Processor agrees:
		1. to store and process personal data securely and destroy it confidentially when it is no longer necessary and instructed by the Data Controller.
		2. to return to the Data Controller any personal data held at the end of the contract, ensuring secure transfer, or to make arrangements for its secure disposal upon the instruction of the Data Controller.

**Data Processing Contract between the Data Controller and the Data Processor**

On behalf of the Data Controller:

Name……………………………………………………………………………

Signed……………………………………...............Date………………..……

Name…………………………………………Position……..…………………..

(Print name & position of authorised signatory)

On behalf of the Data Processor:

The Provider………………………..…………………………………

Signed……………..……………………………..…Date………………..………

Name…………………………………………Position……………………………

(Print name & position of authorised signatory)

**SCHEDULE 1**

The Data Controller [insert healthcare business name] wishes to engage the services of the Data Processor [insert name of provider] to process personal data on its behalf under the terms and conditions of this contract for the purposes of:



**DEFINITIONS**

**Personal data** –any factual information or expressions of opinion relating to an individual who can be identified directly from that information or in conjunction with any other information coming into the possession of the data holder.

**Data Controller** –the individual or organisation that decides the purpose of processing personal information, including what information will be processed and how it will be obtained.

**Data Processor** –an individual (other than an employee of the Data Controller) or organisation that processes personal information while undertaking a business activity or contracted service on behalf of the Data Controller.

**Data Processing** –any business activity or contracted service that involves using personal, corporate or other information for any purpose, including obtaining, recording, holding, viewing, storing, adapting, altering, deleting, disclosing. This is not restricted to computer processing, but includes manual files and verbal discussions.