**Data Sharing Agreement – Controller to Controller**

**Guidance Notes**

It is not a legal obligation to have a contract such as this in place in a controller-to-controller relationship. However, the ICO has stated that it would be ‘best practice’ to do so, and in handling data breaches that involve disputes between the two controllers, such as a medical professional and the hospital in which the healthcare care professional is affiliated with. It is in your best interest as data controller to have an agreement in place with any public or private hospital or clinic in which you are affiliated with to govern matters in the event of a data breach, such as where a patient’s medical records have gone missing.

**Controller to Controller Data Sharing Agreement**

**Between**

**[INSERT HEALTHCARE PROFESSIONAL NAME]**

**Registered Data Controller Reference Number [INSERT NUMBER]**

**And**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Registered Data Controller Reference Number [INSERT NUMBER]**

**Date of Agreement: [INSERT DATE]**

**Introduction**

The parties to the agreement routinely work together to advise, provide expertise to or treatment to patients [CHANGE IF NECESSARY] of [INSERT NAME OF OTHER DATA CONTROLLER] in healthcare matters. The exchange of information facilitates this partnership and must always adhere to legal requirements such as the UK General Data Protection Regulation (UK GDPR).

For the purposes of this agreement both Parties handle and process personal data and sensitive personal data as defined in the UK GDPR as Data Controllersin their own right.

**Between**

This Data Sharing Agreement (“Agreement”) dated [insert date] is between:

a) [INSERT NAME] as Data Controller

and

b) [INSERT NAME] as Data Controller.

This Agreement is supplemental to any other separate contract or data sharing agreement entered into between the Parties and exists to ensure that there are sufficient security guarantees in place for the safe sharing of personal data and sensitive personal data in accordance with the UK GDPR.

Information to which this Agreement relates must be handled in accordance with the appropriate legislative and regulatory environment and each Party’s relevant policies and procedures.

**Commencement of Agreement**

This Agreement will commence at midnight on the date it is signed by the Parties.

**Length of Agreement**

This Agreement will remain in place until terminated by either Party and will apply to all cases upon which the Parties work together, and to all patients with which the Parties work together, now and in the future, unless expressly stated otherwise.

**Definitions**

For the purposes of this Agreement, “Relevant Information” shall mean any or all personal or special category data relating to a patient or his/her case on which the parties are working together as defined by the UK GDPR.

**Purpose and Objective(s) of the Data Sharing**

The purpose of the sharing of data detailed in this Agreement is to provide healthcare advice and/or treatment to the patient or patients.

**Transfer and Frequency of Data**

Relevant information will be shared as and when required in order for both Parties to discharge their responsibilities to the patient and run the matter appropriately.

Relevant information will be shared on a strict need-to-know basis only and will only be processed by staff of either Party in order that they can perform their duties in accordance with one or more of the defined purposes.

**Access and Security**

Under no circumstances should relevant information be left unattended or processed in any way that is unsecure.

Each Party shall ensure they have implemented appropriate security measures, including, but not limited to:

* ensuring all working electronic devices are encrypted;
* ensuring any portable media (such as CDs, DVDs, USB flash drives etc.) which contain the relevant information are encrypted; and
* ensuring attachments containing sensitive personal data being shared via emails are all encrypted and password-protected.

Each Party shall notify the other Party immediately if they become aware of any unauthorised or unlawful processing, loss, damage or destruction of the relevant information. This includes any ‘near-misses’ and any incidents reported to the Information Commissioner’s Office (the ICO). It is the responsibility of the party managing the incidents to investigate, report and escalate them as appropriate to the necessary regulatory bodies.

Each Party shall ensure that any processor, agent or subcontractor instructed by them to process relevant information to which this Agreement relates will process such information in accordance with the UK GDPR and that all appropriate data sharing or processing agreements or contracts are in place.

Each Party will ensure that all staff with access to the relevant information have received appropriate data protection or information governance training and are aware of the confidential nature and duties placed on those processing such information. This includes ensuring they have appropriate monitoring policies and procedures in place for all staff.

Failure to meet the standards within this Agreement will result in Relevant Information not being shared, which could result in the termination of this and other service agreements.

**Processing of the Information**

Each Party remains responsible for the relevant information they hold and process (once safely received) from the other Party as data controller of that information.

Each Party will ensure the relevant information will not be processed outside of the UK without the appropriate safeguards being in place to satisfy the UK GDPR.

Each Party will comply fully with the UK GDPR and other relevant legislation. Particular attention must be paid to the obligations ensuring the security of the relevant information and systems. Each Party will protect such information from unauthorised or unlawful processing, accidental loss, destruction or damage, and acknowledges that they have implemented the required technical and organisational measures.

**UK General Data Protection Regulation (UK GDPR) and Freedom of Information (FOI) Act**

Each Party is responsible for complying with complaints, queries and objections regarding relevant information sharing, subject access and freedom of information requests directed to their organisation in line with the relevant legislation or policies in practice. Each individual request must be dealt with on a case-by-case basis and the consequences of their decisions (for example, to object to sharing) must be clearly explained to the individuals in writing by the party receiving the request.

**Retention Periods**

Relevant information will be retained in line with each Party’s data retention policy, which both Parties confirm meets the requirements under the UK GDPR.

**Disposal of Information**

Both Parties are individually responsible for deleting or safely disposing of the relevant information when it is no longer required in line with their own data protection policies, which meet the requirements of the UK GDPR.

**Termination and Variation**

Any Party may leave this Agreement by giving thirty (30) calendar days’ notice in writing to the other Party/Parties. The terms of this Agreement remain binding on any information shared and retained throughout its lifecycle, irrespective of whether the Party remains a current signatory to this Agreement.

Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to key contacts within each Party so that the impact of the proposed changes can be assessed.

No variation of the Agreement shall be effective unless the Agreement is amended, and it is signed by all Parties.

This Agreement shall be governed and construed in accordance with [English] law and the Parties agree to submit to the exclusive jurisdiction of the Courts of [England and Wales.]

Signature

[INSERT NAME]

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date