## INFORMATION SHARING PROTOCOL

### Title of Agreement

<table>
<thead>
<tr>
<th>Organisation Name</th>
<th>Head Office Address</th>
<th>Telephone</th>
<th>Email</th>
<th>ICO Registration reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essex University Partnership NHS Foundation Trust</td>
<td>The Lodge, Lodge Approach, Runwell Wickford Essex SS11 7XX</td>
<td>01268 407737</td>
<td><a href="mailto:Epunft.info.gov@nhs.net">Epunft.info.gov@nhs.net</a></td>
<td>ZA242481</td>
</tr>
</tbody>
</table>

### Version Control

<table>
<thead>
<tr>
<th>Date Agreement comes into force</th>
<th>Date of Agreement review</th>
<th>Agreement owner (Organisation)</th>
<th>Agreement drawn up by (Author(s))</th>
<th>Status of document – DRAFT/FOR APPROVAL/APPROVED</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**: DO NOT USE
Information Sharing Protocol

1. Purpose
The parties have entered into this Information Sharing Agreement to facilitate and enable the smooth transition of Information Sharing between them. The Information Sharing Agreement is a requirement of the DSPT and also meets the best practice guidance of the Information Commissioner’s Data Sharing Code of Practice. This could consist of data being transferred just once or on an ongoing regular basis, as agreed by the parties involved.

Benefits to the patient will include:

Benefits to the patient will include timelier sharing of information between EPUT and …………

2. Information to be shared

The types of information listed above is not exhaustive and additional information can be shared if certain criteria is met and this will be considered on a case by case basis, as appropriate.

3. Legal Basis for Sharing information

The purpose of this information sharing agreement is to provide a detailed process for information sharing between/for the ………….. service/organisations.

This information Sharing Agreement is entered into for the purpose of the parties sharing information as required or permitted under the data protection legislation and any other relevant legislation which shall include (but not limited to):

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Freedom Of Information Act 2000
- Human Rights Act 1998
- Mental Health Act 1983
- Health and Social Care Act 2012
- Mental Capacity Act 2015
- HSCIC Guide To Confidentiality
- Information Governance/Caldicott 2 Review: to share or not to share
- Records Management NHS Code or practice
- NHS England Safe Haven Procedure
- NHS Constitution
- Information Security Management: Code Of Practice
The parties acknowledge and agree that they will share information whenever either or both parties are under a statutory duty to do so. In this case, the party requesting the information shall make clear in its Data Securing Request the legislation underpinning the request for information and the disclosure of information shall comply with the relevant legislation and be made in accordance with the terms of this Information Sharing Agreement, if applicable.

The parties acknowledge and agree that they will not be bound by the terms of this Information Sharing Agreement in the event either or both of them are prohibited to share information by any legislation.

If consent is deemed to be required for the sharing of personal data, this will be a transparent process.

Where it has been identified that the parties are permitted to share information without obtaining consent, this should be justified, if required, under their statutory or legal powers. Data subjects should be made aware of this decision and provided with the details of the data share, unless, by doing this will risk harm to others or hinder any investigation or legal proceeding.

The decision to share information without consent will be fully documented and held within the patients ‘care record’.

It is good practice to seek freely given, specific, informed and valid consent of individuals to share their information. However disclosure may be lawful in certain circumstances without consent, for example the performance of public functions, legal obligations, prevention/detection of crime.

(Explain the legal power(s) you have that allow you to share the information – include how the sharing is consistent with the General Data Protection Regulation 2016 (GDPR)).

<table>
<thead>
<tr>
<th>Personal Data</th>
<th>Special Categories of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing personal information in accordance with this protocol is lawful under the General Data Protection Regulation 2016 article 6(dropdown)</td>
<td>Sharing personal information in accordance with this protocol is lawful under the General Data Protection Regulation 2016 article 9: (if appropriate): [please complete]:</td>
</tr>
<tr>
<td>Vital Interests</td>
<td>Article 9(2)(h)</td>
</tr>
<tr>
<td>Legitimate Interests</td>
<td></td>
</tr>
</tbody>
</table>
Other legislation or statute as follows
Children’s Act 2004, Section 10 & 11- Cooperation to improve well-being.
Children’s Act 1989. Part III: Section 17 (1) (provision of service)

Fair Processing in accordance with General Data Protection Regulation 2016 article 12.

<table>
<thead>
<tr>
<th>Fair processing requirements have been satisfied by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information of both parties’ Fair Processing Notices being either fully available on their respective publicly available websites or available on request (via electronic or hardcopy):</td>
</tr>
</tbody>
</table>

The information listed above will be available to the data subjects in the following methods:

- Your health records: what you need to know (EPUT leaflet)
- Your health records: what you need to know (EPUT Poster)
- ...
- ...

4. Access and individuals’ rights

(Explain what to do when an organisation receives a DPA or FOI request for access to shared data).

Subject Access is an individual’s right to have a copy of information relating to them which is processed by an organisation.

Once information is disclosed from one agency to another, the recipient organisation becomes the Data Controller for that information. With regards to subject access requests, the Data Controller has a statutory duty to comply with Article 15, unless an exemption applies. It is good practice for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual.

If a party receives a request for information under the Freedom of Information (FOI) Act [2000] that relates to data that has been disclosed for the purposes of this Information Sharing Protocol, it is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption under the provisions of the FOI Act and to identify any perceived harms. However, the decision to release data under the FOI Act is the responsibility of the agency that received the request.
5. Keeping information secure

All information shared between the parties involved in this ISP will be held in a secure location with limited access and used only for the purposes listed in this agreement.

- Each party shall ensure that access to information provided by the other party under this ISP will only be granted to those staff who ‘need to know’ the information.
- The information shared between the parties must not be disclosed to any third party.
- All information held on portable devices must be encrypted to industry standard FIPS 140-2/256-bit asymmetrical encryption.
- All data will remain and be stored on servers physically located within the United Kingdom.

Security for the exchange of information will be achieved through a secure - fill in exchange type (e.g. secure site, secure nhs.mail to nhs.mail).

Partners receiving information will:

- Ensure their employees can only access the shared information appropriate to their role;
- Ensure that their employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
- Protect the physical security of the shared information.

6. Information format and frequency of sharing

The format the information shared is either in - insert format type here (e.g. Microsoft excel or csv file).

The frequency with which the information will be shared is a (………………) transfer of information.

7. Data Retention

(Include detail here how long each organisation will retain the information for).

Information will be retained in accordance with each partners’ data retention policy and in any event no longer than is necessary.

For the purposes of this agreement, destruction means that data must be irretrievable following destruction or deletion, in accordance with ISO27001 international standard for information security.

The controller will retain information in accordance with the Department of Health’s retention of records schedules.

The processor must not make multiple copies of the data.
The processor shall ensure that the destruction of data will also take place for backup media and provide written confirmation to the controller when destruction has taken place.

8. Responsibility for exchanging these data and ensuring data are accurate

Each of the data providers will ensure the accuracy of the data being shared using their own internal quality assurance checks.

For the purposes of this Protocol the responsibilities are defined as:
Caldicott Guardians and Senior Information Risk Owners (SIRO) who have signed the Information Sharing Agreement as having overall responsibility within their own organisation have the duty for ensuring the organisation has the necessary powers to share the information requested. Any information shared must only be used for the purpose as requested.
The parties in discharging their obligations under this information sharing agreement shall comply with the eight data protection principles.
The parties shall ensure that the information shared is relevant and proportionate to the purpose for which it is shared and will comply with the Data Protection Act, information will not be passed to any third party other than allowed by law, retention for the intelligence purposes shall be allowed but only in line with the Data Protection Act.

EPUT have/have not undertaken a privacy impact assessment as under this information sharing agreement information will be shared only where the parties are legally required or permitted to do so.
All parties involved have agreed that the service users (data subjects) need to be informed of the following:

- What information is going to be shared
- In what format is the data going to be exchanged
- Who the information is going to be shared with
- For what purposes it will be used

Unless by doing so would risk harm or self to others or hinder any investigation or legal proceedings.

Data Controllers for this Protocol are:
Joint Data Controllers for this Protocol are:

[“Joint” covers the situation where the determination is exercised by data controllers acting together, typically with written data controller agreements setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied. The participation of the parties may take different forms and need not necessarily be equally shared across all aspects of the processing. Their contributions may be sequential or simultaneous and their liability if something goes wrong may differ.]

Data Controllers in Common for this Protocol are:

[“In common” is where data controllers share a pool of personal data, often disclosing data to each other but with each processing the data independently of the other(s). As with ‘joint’ arrangements, data controllers in common should have written agreements and processes for ensuring that all data controller responsibilities are satisfied. Each needs to exercise due diligence in ensuring that all parties involved are meeting the requirements of law.]

Data Processors are:

[A data processor can be anyone (other than an employee of the data controller) who processes the data on behalf of the data controller. The Act imposes specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors.

Where Data Processors are a part of this Protocol, the data controller retains full responsibility for the actions of the data processor — if there is a data protection breach then the data controller remains responsible. The key obligation is that the processing by a data processor must be carried out under a written contract which requires the data processor to act only on instructions from the data controller. In the absence of a written contract a Partner to this protocol will be a data controller in its own right and will need to meet all the requirements of the Data Protection Act 2018 and the General Data Protection Regulations 2016.

9. Complaints

Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.

10. Breach of Confidentiality

(Provided detail here of what the expectation in the event of a breach of the data sharing initiative. Including who should be contacted and reporting timescales).

Any reported potential or actual breach of security or inappropriate / unauthorised disclosure of data will be investigated. It is the responsibility of the Data Provider to report the incident following its own internal reporting processes for data breaches.
11. **Agreement**

We undertake to implement and adhere to this protocol.

Signed by Governance Lead
Print:……………………………………………………………………………………

Signed:……………………………………………………………………………………
On behalf of
(Organisation):………………………………………………………………………

Signed by Governance Lead
Print:……………………………………………………………………………………

Signed:……………………………………………………………………………………
On behalf of
(Organisation):………………………………………………………………………

Signed by Governance Lead
Print:……………………………………………………………………………………

Signed:……………………………………………………………………………………
On behalf of
(Organisation):………………………………………………………………………
<table>
<thead>
<tr>
<th><strong>Definitions</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>DPA</td>
<td>The Data Protection Act</td>
</tr>
<tr>
<td>FoIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td><strong>Personal Information</strong></td>
<td>“Personal Data” as defined in the above DPA GDPR</td>
</tr>
<tr>
<td><strong>Personnel</strong></td>
<td>Partner organisations’ employees, officers, elected members, directors, voluntary staff Consultants and other contractors and their sub-contractors</td>
</tr>
<tr>
<td><strong>Sensitive personal data</strong></td>
<td>As defined in the above DPA GDPR</td>
</tr>
<tr>
<td><strong>Service users</strong></td>
<td>Recipients of the partner organisations’ health and care services. Also known as “data subjects” within the meaning of the DPA 2018 / GDPR</td>
</tr>
<tr>
<td>ISA’s</td>
<td>Information Sharing Agreements</td>
</tr>
<tr>
<td>PIA/DPIA</td>
<td>Privacy impact assessments</td>
</tr>
<tr>
<td>SIRO</td>
<td>Senior Information Risk Owner</td>
</tr>
<tr>
<td>Data Privacy Impact Assessments</td>
<td></td>
</tr>
</tbody>
</table>