PRIVACY IMPACT ASSESSMENT FORM

Essex Partnership University NHS Foundation Trust’s (EPUT) data processing activity MUST comply with the General Data Protection Regulation and Data Protection Act 2018.

This Data Privacy Impact Assessment Form will assist Information Asset Owners in identifying how the collection and use of people’s personal data may affect their privacy.

This form should be used for both internal and partnership projects which require the collection and / or use of personal data.

The Information Governance Team will assist in the completion of this form, should it be required and can be contacted as follows:

epunft.info.gov@nhs.net
Tel: 01268 407737/52/55

Timescales for completion of a DPIA are included in the matrix at the end of the form.

SECTION 1

<table>
<thead>
<tr>
<th>(1a)</th>
<th>Project Name / System / Process Change / New Hardware / Software Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What your team will be naming this for recognition. Is this a system / process? <em>(Please delete as appropriate)</em> Is this a change / new system / process? <em>(Please delete as appropriate)</em> Is this hardware / software implementation? <em>(Please delete as appropriate)</em> Is this an access request to one of our systems? <em>(Y/N)</em></td>
</tr>
<tr>
<td>Department</td>
<td>Name of Service / Team / Department</td>
</tr>
<tr>
<td>Lead Officer (Name)</td>
<td>Name of the project lead or person with responsibility for the project / system / process implementation / change</td>
</tr>
</tbody>
</table>
(2a) List all of the agencies that will have access to the personal data collected and used for the purpose/s outlined above:
A list of all the organisations which will be involved with the system / process implementation / change.

(2b) What personal data will be used and why (list all categories)?
A list of all the person / staff identifiable information which might be used within the system / process and give a reason for the use.

(2c) Could the objectives be achieved using Anonymised, Pseudonymised data? (Please tick the Yes / No box. If No is ticked then an explanation is required to justify the use of person / staff identifiable information)

| YES | ☐ |
| NO | ☐ | Explain why: |

(3a) Are there any benefits to the individual of their personal data being used for the purpose/s outlined above? Please describe:
An explanation to tell the reader what the benefits would be to the client / staff for using their information within the system / process. Article 5 (1)(a) of the GDPR “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”
If client / staff information is not used within the system please state “N/A – no client / staff information will be used within the system / process”.

(3b) What are the benefits to EPUT of the individuals’ personal data being used? Please describe:
An explanation to tell the reader what the benefits would be to the Trust for using client / staff information within the system / process. Article 5(1)(a) of the GDPR “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”
If client / staff information is not used within the system please state “N/A – no
### (3c) Are there any negative impacts to the individual of their personal data being used for this project? Please describe:
An explanation to tell the reader what the **negative impacts** might be to the client / staff when using their information within the system / process.
**Article 5(1)(a) of the GDPR** “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”
If client / staff information is not used within the system please state “N/A – no client / staff information will be used within the system / process”.

### (3d) How will you avoid causing distress or damage to the individual when using their personal data for this project?
An explanation to tell the reader what the processes / procedures (physical & written) are in place to ensure distress or damage is not caused to the client / staff when using their information within the system / process.
**Article 5 (1)(a) of the GDPR** “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject” If client / staff information is not used within the system please state “N/A – no client / staff information will be used within the system / process”.

### (4a) Is the data already held by the Trust? (Please tick the Yes / No box.)

| YES ☐ | If so, where / how? An explanation to tell the reader where the information is stored / held and in what form (paper / electric).
| NO ☐ | Which agency will collect the data? An explanation to tell the reader which partner organisation (enter the full name of the organisation) will collect the data if the data is not kept by EPUT.

### (4b) Is the data already held by any of the partner agencies? (Please tick the Yes / No box.)

| YES ☐ | If so, where / how? An explanation to tell the reader where the information is stored / held and in what form (paper / electric) within the partner organisation. **Article 5(1)(f) of the GDPR** “processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures”
| NO ☐ | Which agency will collect the data? An explanation to tell the reader which partner organisation (enter the full name of the organisation) will collect the data if the data is not kept by EPUT.

**Article 5(1)(f) of the GDPR** “processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures”
GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures”

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NO</strong></td>
<td>N/A – information is not kept by any partner organisation.</td>
</tr>
</tbody>
</table>

### (5a) Have the individuals, whose data is being used, been advised it is to be used, how and why you intend to use it? (Please tick the Yes / No box.)

| **YES** | Permission has already been granted – describe how and when: Please state if a consent form has been signed by the client / staff and recorded (when did this take place – was it part of the project plan or prior to the project being undertaken?). (Please send through the consent form template (blank) with the completed PIA form.) |
| **NO** | If not are you intending to tell them, and when? If not, why? An explanation to tell the reader why the client / staff have not been informed. If there are plans in place to notify the client / staff please explain how this will be done and when. Article 5 of the GPDR “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject” |

### (5b) Have individuals been given the opportunity to refuse permission to use their personal data? (Please tick the Yes / No box.)

| **YES** | An explanation to tell the reader if the client / staff have been given the opportunity to say “no” to having their information included within the system / process, if so, when and how? Article 5 (1)(a) of the GDPR “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject” |
| **NO** | If not, why: An explanation to tell the reader why the client / staff have not been given the opportunity to say “no” to their information being included within the system / process. If there are plans in place to give the client / staff this opportunity, please explain how this will be done and when. Article 5 (1)(a) of the GDPR “Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject” |
(6) Is the project / process / system change / new hardware / software required by any statutory / legal obligations? (Please tick the Yes / No box. If Yes is ticked please list the statutory / legal act’s name or guidance name.)

<table>
<thead>
<tr>
<th>YES □</th>
<th>Please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Include an explanation why this is a statutory / legal requirement so that the reader understands the importance of the project – include a copy of the statutory / legal guidance with the completed PIA form.)</td>
</tr>
</tbody>
</table>

| NO □ | N/A |

(7) How will you ensure that all the personal data you are collecting is kept up to date and accurate?

An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information will be kept up to date and accurate.

Article 5(1)(d) of the GDPR “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay”

(8a) How long will the project need to hold the data?

An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information will not be kept for longer than necessary. The Records Management team can be asked for assistance with the length of time you can keep the information before destroying the information appropriately.

Article 5(1)(e) of the GDPR “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of which the data is processed”

(9a) How will the data be held / stored?

An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information is stored and held securely. If this information is held by an external organisation then an explanation of how that organisation will secure the information.

Article 5(1)(f) of the GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures” *(Example – the information will be stored in a limited access folder and only authorised persons will have access. Access will be monitored.)*
### (9b) What security measures will be in place for the held / stored data?
An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information is stored and held securely. If this information is held by an external organisation then an explanation of how that organisation will secure the information.

Article 5(1)(f) of the GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures”

*(Example – Access to the information will be given on a need to know basis and a password and username will be required to access the information system.)*

### (10a) How will the data be shared / transferred between the agencies involved in the project?
An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information is transferred (sent or received) securely. Please state if there is an Information Sharing Agreement in place or an Information Sharing Agreement would be needed to support the process / project.

Article 5(1)(f) of the GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures”

*(Example – Information will be sent / received through NHS mail or the use of a password protected attachment within an Outlook email. The password for the attachment will be phoned through.)*

### (10b) Will the data be transferred to a country outside of the EEA? *(Please tick the Yes / No box. If Yes is ticked please list the Country where the information will be sent. Article 45 (1) A transfer of personal data to a third country or international organisation may take place where there is an adequate level of protection.)*

<table>
<thead>
<tr>
<th>YES</th>
<th>If yes, how?</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>
(11) How will the Trust be assured that third parties will comply with data protection obligations?

(The third party or external organisation must provide the following information because the Trust cannot use the services of another organisation unless they are registered with the Information Commissioners Office)

Party 1
Data Protection Registration Number: ………………………..  
Date Registered: ……………….  Date of Expiry: ………………………...

Party 2
Data Protection Registration Number: ……………………
Date Registered: ……………….  Date of Expiry: ………………………...

EPUT
Data Protection Registration Number: ZA242481
Date Registered: 28 March 2018 Date of Expiry: 27 March 2019

(12) What organisational measures will be implemented to ensure only appropriate and authorised access to, and use of, the personal data?

An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information is accessed appropriately. If this information is held by an external organisation then an explanation of how that organisation will ensure appropriate access.

Article 5(1)(f) of the GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures”

(Example – Access to the information will be given on a need to know basis and a password and username will be required to access the information system.)

(13) How will technical / organisational security, in relation to this project, be monitored / audited?

An explanation to tell the reader what the process or procedure (physical & written) will be to ensure that the client / staff information is monitored or audited. If this information is held by an external organisation then an explanation of how that organisation will monitor access.

Article 5(1)(f) of the GDPR “processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures”

(Example – Confidentiality audits will be carried out on a monthly basis.)
Please confirm whether a Business Continuity Plan is in place for this proposed new process / system?

Please tick the **Yes** / **No** box. If Yes is ticked, please send the Business Continuity Plan document with the completed PIA form. If **No** is ticked, please detail what processes / procedures have been put in place to ensure that the service / team / department is not disrupted / stopped if the system / process fails or is inaccessible.

**YES** □ (please attach)
**NO**.... □ (please explain how the work will continue in the event of a failure)

The lead officer for the project / system / process / hardware / software implementation / change should complete the following:

> As lead officer I confirm that the information recorded on this form is to the best of my knowledge an accurate and complete assessment of the potential privacy impacts of this project:

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESIGNATION</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Project Lead</td>
<td>Job Title of Project Lead</td>
<td>Signature (Electronic Signature can be used)</td>
<td>Date of Signature</td>
</tr>
</tbody>
</table>

**SECTION 2 (FOR USE BY THE INFORMATION GOVERNANCE TEAM AND APPROVING PERSON / GROUP / COMMITTEE)**

The completed form should be passed to the Information Governance Team for comments / recommendations then forwarded to the appropriate Trust committee for approval / action planning.

Privacy Impact Assessment reviewed and approved on behalf of the IG Team/DPO

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESIGNATION</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
</table>
Privacy Impact Assessment reviewed and approved on behalf of the Information Governance Steering Sub-Committee:

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESIGNATION</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information Governance Team / Committee comments / recommendations regarding the proposed projects’ compliance with the General Data Protection Regulation/Data Protection Act 2018:

PIA Reference Number (completion by IG Team only): PIA000

Approving Committee / Group

The Committee / Group has considered the PIA with the following recommendations:

- 
- 

and approves the implementation of (Project Name):

Date: ______________ Signed (Chair): __________________________
### SECTION 3 - Timescales for completion of PIA:

<table>
<thead>
<tr>
<th>Action</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template sent to Project Lead for completion &amp; return to IG Team</td>
<td>n/a</td>
</tr>
<tr>
<td>Advice &amp; recommendations returned to Project Lead for updating</td>
<td>1 week (repeated as necessary)</td>
</tr>
<tr>
<td>Updates completed – IG Team submit final draft as follows:</td>
<td></td>
</tr>
<tr>
<td>· PIA confirms no person identifiable / corporately sensitive data involved / no impact on Trust – Head of Information Governance approval only required</td>
<td>+ 1 week</td>
</tr>
<tr>
<td>· Person identifiable / corporately sensitive data involved / impact on Trust – Information Governance Group / Chairs’ approval required</td>
<td>+ 1 month</td>
</tr>
<tr>
<td>· Patient identifiable data involved – Caldicott Network / Chairs’ approval required</td>
<td>+ 1 month</td>
</tr>
</tbody>
</table>