NHS
East London
NHS Foundation Trust

Data Protection Impact Assessment (DPIA)
Template

A Data Protection Impact Assessment (DPIA) must be completed whenever a new service, process or information asset is introduced or there is a change to an existing process or service. Steps 1 – 3 must be completed for all projects / proposals. If advised to do at the end of Step 3 please complete Step 4. Completed DPIAs should be emailed to elft.information.governance@nhs.net

Step 1. Project / proposal details *Complete for all projects / proposals*

Project / proposal name: **Implementation of a Primary Care Webpage for staff.**
Description of project / proposal: Explain broadly what project aims to achieve and what type of processing it involves. Please attach a document or link to other documents, such as a project proposal if you have one. Is it a new electronic system, service acquisition, software, information sharing proposal or something else? **Following feedback received from staff across primary care, staff reported that it was not always possible to access key documents and information from the Trust Intranet due to connectivity issues. Some sites do not have access to the Trust network due to server issues. As a result the Directorate Management Team agreed to set up a webpage for Primary Care staff which can be accessed via any internet platform and does not rely on Trust PC/system access. This would also allow all primary care documents to be stored in one place.**
Give an overview of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? Attach a flow diagram or describe data flows. What types of processing identified as likely high risk are involved? **Staff will have access to the webpage via a user name and password (we can use nhs.net as user name but will need a new password).** **Information to be made available – policies, procedures, leaflets, posters, reports quality & performance, education videos, comms using you tube/podcasts, link to twitter, training material, link to report incidents (Datix).**
Is a supplier involved in the processing? If the supplier is known at this stage, give supplier details – attach evidence of DSPT accreditation, BS27001 accreditation or otherwise copies of their information security policies, evidence of IG training etc **Winona Esolutions is being used to create the page, this supplier is already on the Trust approved list and also set up the Trust Intranet.**
What are the benefits? - **Improve accessibility for staff to access key information, documents, messages** - **Ability to link to key systems such as Datix to allow staff who do not have access to Trust site to report incidents** - **Fun and interactive videos / podcasts from staff across primary care – help staff to stay connected** - **Store training material – slides / handouts** - **Store policies and procedures local to primary care – SOPs / Handbook**

- **Access to reports such as quality, performance, KPIs, compliance**
Proposed implementation date: 1st March 2021

Step 2. Contact details *Complete for all projects / proposals. Please contact the IG team if anything is unclear*

Work stream lead / project manager details	
Name **Charan Saduera**	**Job title** **Associate Director for Quality, Compliance & Performance CHS**
Email **Charan.saduera@nhs.net**	**Phone** **07920214351**
Information Asset Owner (if different from above). This will be a Service Director, Corporate Director / Associate Director	
Name **Dr Liz Dawson**	**Job title** **Medical Director**
Email **liz.dawson1@nhs.net**	**Phone** **07811 208881**
Information Asset Administrator (or System Owner). This will usually be a team manager, IT super user etc	
Name **Marina Muirhead**	**Job title** **Director of Primary Care**
Email **marina.muirhead@nhs.net**	**Phone** **07717418219**
Executive Director sponsor details. Required for large scale change, acquisitions etc, not for small projects	
Name: **Dr Mohit Venkataram**	**Job title:** **Executive Commercial Director**
Email **mohit.venkataram@nhs.net**	**Phone** **02076554260**

Step 3. Screening questions. *Complete for all projects / proposals*

Answering YES to any of the screening questions represents a potential high risk to the rights and freedoms of individuals and therefore a full DPIA must be completed to ensure those risks are identified, assessed and fully mitigated.

Screening questions	Yes or No
Will the project / proposal involve the collection / processing of information about individuals? (this could be service users, carers, staff, stakeholders etc)	**No**
Does it introduce new or additional information technologies that can substantially reveal business sensitive information / have a high impact on the business?	**No**
Will it require individuals to provide information about themselves?	**No**
Will information about individuals be disclosed to organisations / individuals who have not previously had routine access to the information?	**No**
Will information about individuals be used for a new purpose or in a new way?	**No**
Does it use technology that could be seen as intrusive e.g. automated decision making?	**No**
Will it result in making decisions about individuals that may have an impact on them e.g. research, service planning, commissioning new services?	**No**
Will it change the delivery of an individual's direct care?	**No**
Will it require you to contact individuals in a way they might find intrusive?	**No**
Does it involve any other organisations?	**No**
Does it require individuals to consent to their information being processed?	**No**
Does it involve new or significantly changed handling of a considerable amount of personal / business sensitive information about an individual in a database or system?	**No**
Does it involve new or significantly changed consolidation, interlinking, cross referencing, or matching of personal / business sensitive data?	**No**
Does it use cloud services / is it stored in 'the cloud'?	**Yes**
Is it about children or vulnerable groups of adults e.g. service users?	**No**
Will it be used for research purposes / projects?	**No**

If you answered YES to any of the above questions please complete Step 4. If you answered NO to all questions then please send your DPIA to elft.information.governance@nhs.net. We will assess your request and either confirm our data protection support for your project / proposal or request further information. Please contact the IG team if anything is unclear.

<u>Step 4. Full Data Protection Impact Assessment</u> *Complete only when advised a full DPIA is necessary at the end of Step 3*

4.1 Processing
What data will be collected / processed? Does it include health or any other special categories of data? If so, please list. These are health, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **The page will only include Trust documents such as policies, procedures, leaflets, Trust videos/podcasts, training material, reports local to primary care such as quality and performance.**
How will the data be collected? **From local teams and trust systems**
Where will it be collected from? **Local teams, Trust depts such as training compliance / patient feedback / performance / assurance, partner organisations for comms e.g. CCG.**
What will it be used for? **For staff to access to support them in their role/running of service**
Will it be processed manually? Yes or No **No**
Will it be processed electronically? Yes or No **Yes**
How is access controlled? For example passwords, Smartcard, locked door **The page will have a data controller who will have access to the back end of the system to upload new or updated information and monitor version control.**
Will only the minimum data necessary be collected / stored / processed? **Yes**
Will be anonymised, pseudonymised or collated with other data? **No**
Will any third parties access the data? Who? For example if another organisation wants access to our systems **Winona Esolutions (Trust approved list who has set up the Trust intranet page).**

Will it be sent off site or shared externally i.e outside the Trust or outside its computer network? Yes or No **Yes as the access for the page will be via secure Extranet however, access is restricted to approved account holders in ELFT.**
If sent off site, where to? Name the other agency / company / location / country **Winona Esolutions (UK) and service centre is UK based. UK South service.**
If so, is there a contract / data controller to processor agreement, information sharing agreement? If yes, please attach **Yes hosting contract already in place with ELFT.**
How will it be sent? **We will upload resources to the Extranet.**
How long will the data be retained in identifiable form? **Once the contract ends the data will be destroyed covered until end of 2021.**
Will it be de-identified or destroyed. How? **Drives will be wiped.**
Are you aware of any concerns or risks over the processing / use of the data, system, supplier, other agency etc? **We are using a Trust approved supplier to build the webpage and are not aware of any new concerns or risks with this web developer.**
Has any / will any consultation take place? Yes or No? Please list, also include feedback received **One initial meeting has taken place Dec2020 with the developer to discuss the project and its requirements.** **Further meetings will be set with the design group to agree content of webpage.**

4.2 Cloud considerations. You must complete this if you answered Yes in Step 2 to 'Does it use cloud services / is it stored in 'the cloud'?
Which country is the cloud provider based in? **UK.**
Is the cloud service hosted on HSCN? **No.**
What business continuity plans are in place if the provider ceases trading? **Contract will be up for renewal in 2021 (Annual rolling contract). Company will create an archive which will allow us have access our information / docs. Confirmation is given before deleted**.
What secure arrangements are in place at the end of the contract with the cloud provider to transfer the data? **Company will create an archive which will allow us have access our information / docs. Confirmation is given before deleted.**
Who would legally own any data uploaded to the cloud application by the Trust? **ELFT – primary care**
What information & cyber security policies does the cloud provider have? Please attach information / embed a link **To be sent via email**

Please send your completed DPIA to elft.information.governance@nhs.net. We will assess your request and either confirm our data protection support for your project / proposal or request further information.

Information Governance assessment

To be completed by the information governance team who will advise you once the assessment is complete

Compliance area	Assessment of compliance	Compliance agreed by IG Manager Y / N
Principle 1 Lawfulness, fairness and transparency Transparency: Are data subjects aware what data processing will be done? Fair: Is the processing as described? Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)], that personal data shall be: "(a) processed lawfully, fairly and in a transparent manner in relation to individuals		
Principle 2 Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Is the data only being used for the specific processing purpose that the subject has been made aware of?		
Principle 3 Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. Is only the minimum amount of data kept for specific processing?		
Principle 4 Personal data shall be accurate and, where necessary, kept up to date. [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Are there rectification processes in the data management / archiving activities		
Principle 5 Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than		

<table>
<tr><td>necessary” [article 5, clause 1(e)]. Is this recognised and what processes are in place to ensure it happens?</td><td></td><td></td></tr>
<tr><td>Principle 6
Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage” [article 5, clause 1(f)]. Is the security adequate? Is there a system level security policy?</td><td></td><td></td></tr>
<tr><td>Information sharing
Is an information sharing or third party access agreement required? Y/N</td><td></td><td></td></tr>
<tr><td>Cloud considerations
Has the Information Security Manager approved the Cloud section? Y/N</td><td></td><td></td></tr>
<tr><td>Risks
Assess the source of risk & nature of potential impact on the rights & freedoms of individuals. Include associated compliance & corporate risks as necessary</td><td>
<table>
<tr><td></td><td colspan="5">Likelihood</td></tr>
<tr><td>Severity</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td></td><td>Rare</td><td>Unlikely</td><td>Possible</td><td>Likely</td><td>Almost</td></tr>
<tr><td>5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
<tr><td>4 Major</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>3 Moderate</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>2 Minor</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>1 Negligible</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
</table>

Is the risk great enough to report to the ICO? Y/N

Add comments:</td><td></td></tr>
<tr><td>Asset register / data flows mapping
Has the asset been added to the relevant asset register? Y/N</td><td></td><td></td></tr>
</table>

Information governance team to forward to DPO

Data Protection Officer approval

DPO comments

DPO approval granted? Y/N
DPO name:
DPO signature:
DPO approval date:

DPO to return form to information governance team for documenting and returning to project manager

Date returned by IG team to project manager: