Data Protection Impact Assessment – NHS Confederation

This template follows the process set out in the ICO's guidance for undertaking a Data Protection Impact Assessment (DPIA), and you should use it alongside that guidance which can be accessed on their website here: ICO - Data Protection Impact Assessments Guidance

The template should be completed at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process, and the final outcomes should be integrated back into your project plan.

Please contact the data protection lead (Penny Coombes) if you need further guidance to complete the DPIA by emailing dataprotection@nhsconfed.org

Step 1 – Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The project will be to build a Candidate Monitoring Tool for the Step into Health programme. This enables members of the Armed Forces community to register with the programme, enter their job requirements and be connected to employers in their region. This also helps our employers to track their engagement with this community, recording their conversations, any work placements and what the outcomes of these are. NHS Employers will have access to all data for reporting and administration purposes. This project will process candidate's contact and Armed Forces community employment data. The associated data and processing does not represent a high risk to the rights and freedoms of individuals concerned (see link to ICO DPIA). Thus a DPIA is not necessary or will need to be shared with the ICO. However, NHS Confederation project initiation processes request a DPIA to be completed to ensure data protection risks are considered and "Privacy by design" is built into the project plans.

Step 2: Describe the processing

Describe the nature 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? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
See file below for project scope. CANDIDATE MONITORING TOOL The data from the Armed Forces community will be provided by the user when registering, this will include:

- Name, contact details, Armed Forces community description (veteran, service leaver, spouse, dependant, cadet), service number (for veterans & service leavers), rank, military branch (Army, Navy, RAF, Royal Marines), date of leaving or date available, current location, location of interest, job type, role areas of interest, looking for (work placement, job opportunities, apprenticeships, interview support, application support), source of referral (event, individual contact, social media, referral through charity).

Employers will be able to record their engagements with individuals including:

- Details of phone calls
- Work placements
- Event meetings

Employers will be able to refer candidates to other employers via email, although no data will leave the system, they will receive a notification prompting them to log into the tool.

Employers having access to the tool will be required to complete a data sharing agreement.

NHS Employers will have control of who has access to the data and this will be reviewed on a 6 monthly basis.

No high-risk data processing will be undertaken.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

No special or criminal offence data is stored.

The numbers of people expected to register with the people is unknown at present but based on our average web hits per month this could be in the thousands. Users will have full control to edit and close down their data at any time. This will then delete their personal information but for reporting purposes, a ghost account with the outcomes of their engagement/non-personal data will endure. A data retention policy will be agreed as by the project team.

The tool is open to anyone serving or past member of the UK Armed Forces and their families (18 years and above).

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

This project does not process data from children or vulnerable groups or involve processing data in a novel or insecure way. The legal basis for processing will be legitimate business interest and the subjects will be able to request processing to cease at any time.

A Privacy Notice will give details of how their data will be processed and shared.

The Assurance Board reviewed the proposed tool and provided full sign off – no concerns were raised throughout the process. There were no existing tools that provided us with what we were looking for hence the bespoke build.

Information entered into the system will be voluntarily provided by the individual and they will retain full control over the edit and deletion of their record (as above).

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step into Health provides an access pathway to the NHS for those individuals from the Armed Forces community. We work with employers to support them embed recruitment activity to do this. Our contract to lead Step into Health nationally runs until end March 2020 and we are currently in discussion to extend this. The programme is funded through 4 sources – NHS England, NHS Improvement, NHS Leadership Academy and the Royal Foundation. It has a governance structure comprising an Assurance Board and a Stakeholder Reference Group.

We want to ensure the tool provides a more robust reporting mechanism for NHS Employers and our employers. We want to provide a better experience for those from the Armed Forces community taking part in the programme.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: identify who the stakeholders are. Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

We have convened a task and finish group including members of the Step into Health programme team and employers. They will be utilised through building the spec, the tender process and testing phases.

We have a network of members of the Armed Forces community who will be used during testing phases.

Our Assurance Board provide final sign off for the tool including spec, budget and final option.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The legal basis for processing will be legitimate business interest and the subjects will be able to request processing to cease at any time. A Privacy Notice will give details of how their data will be processed and shared and provide details of their rights.

Data is held securely on UK based servers.

Employers having access to the tool will be required to complete a data sharing agreement which will be actively managed for the duration of the project.

We will only request data to be input from those areas that are needed to ensure we meet our aims. The data requested has been devised by our task and finish group over several weeks.

Only specific outcomes listed in the document will be recorded and reported on.

The individual's data will be kept up to date by them and they have full ownership. On registration individuals will be asked to agree to the relevant statements provided by our GDPR officer and all employers will be required to sign a data sharing agreement, updated every 6 months.

We will monitor the usage of the tool in-house and provide help/support to all users with the tools designers available to make any changes on a bill-back basis.

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall Risk** Low, medium or high
Data breach – reveal location and personal details of users of the system.	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced or accepted	**Residual risk** Low, medium or high	**Measure approved** Yes/no
Data breach	Specification in contract to website builders to use appropriate technical measures.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name / Date**	**Notes**
Measures approved by:	Gemma Wright – March 2019	*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:	Gemma Wright – March 2019	*If accepting any residual high risk, consult the data protection lead before going ahead*

<table>
<tr><td>Data protection lead advice provided:</td><td>Rob Stead – June 2019</td><td><i>Data protection lead should advise on compliance, step 6 measures and whether processing can proceed</i></td></tr>
<tr><td colspan="3"><b>Summary of data protection lead advice:</b>
DPIA is unnecessary but has been completed as good practice. Final document includes advice in each section. To summarise;
1. The data being processed does not represent a high risk to the rights and freedoms of individuals.
2. Need data sharing agreement with each Employer.
3. Legal basis of processing will be legitimate business interests.
4. Privacy notice should be clear and accessible.
5. Subjects may request processing to cease and have personal data deleted.
6. Appropriate security measures should be built into the Tool.</td></tr>
<tr><td>Data protection lead’s advice accepted or overruled by:</td><td>Accepted by Gemma Wright – July 2019</td><td><i>If overruled you must explain your reasons</i></td></tr>
<tr><td colspan="3"><b>Comments:</b></td></tr>
<tr><td>Consultation responses reviewed by:</td><td></td><td><i>If your decision departs from individuals’ views, you must explain your reasons</i></td></tr>
<tr><td colspan="3"><b>Comments:</b></td></tr>
<tr><td>This DPIA will be kept under review by:</td><td>Gemma Wright/Rob Stead</td><td><i>The data protection lead should also review ongoing compliance with DPIA</i></td></tr>
</table>