NHS
East of England
Ambulance Service
NHS Trust

This template is an example of how you can record your
DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance.

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

Project details

Name of manager completing DPIA	Dean Ayres on behalf of Chris Martin
Title of project	COVAC – COVID 19 Vaccination
Date DPIA completed	06/01/20

Step 1: Identify the need for a DPIA

Explain broadly what 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 aims to achieve the mass vaccination of EEAST staff and associated individuals (those that work in close proximity or in supporting the delivery of service) against the COVID 19 virus. This is task is being carried out as part of the National program/ pandemic plan, which has been coordinated by HM Government, Public Health England (PHE) and the NHS. NHS COVID Vaccination information NHSE Initiation letter Coronavirus (COVID-19) vaccine EEASTs DPIA screening tool has indicated the need to carry out a full DPIA, for the following reasons, the rapid implementation, the collection of health related data and the wide range of data subjects a proportion of which will not be directly employed by East of England Ambulance Service NHS Trust.

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 other way of describing data flows. What types of processing identified as likely high risk are involved?

The data will be collected on 2 existing Trust systems:

The Trusts eLearning Platform Evolve, powered by Totara, this already has the details of all staff and many ancillary workers already within the system and will be used to manage appointment bookings and provide some degree of reporting for reconciliation (internal uses). Part of the data collection on this system will also include the NHS number (which is not currently collected), no health related data will be held on this system.

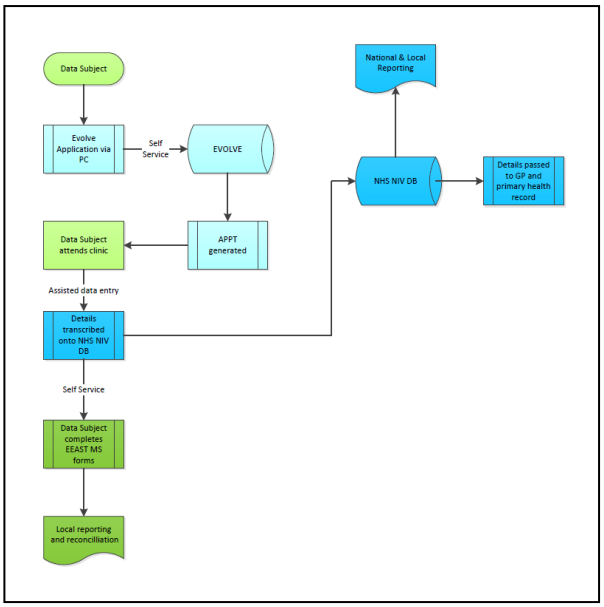
The data held on Evolve is being segregated from the other data allowing for this to be appropriately managed as part of the COPI de-escalation plan.

The second system is MS Forms which is currently being used for lateral flow testing and data is received into an EEAST O265 server and the details are extracted and manipulated within PowerBI (again within the Trusts O365 environment).

The last system (external) is the NHSD NIV, which is the approved National reporting system and will ensure that each data subjects NHS record is updated and the details made available to the appropriate GP (driven by the NHS Number). Anyone who has "opted out" under the National Opt Out Scheme will be managed by NHSD at this point.

The data types being collected on the NHS NIV (NHSD daily immunisation reporting system) system (please see the list of field headings below) and a full description can be found in the NIV Technical Spec

NHS_NUMBER|PERSON_FORENAME|PERSON_SURNAME|PERSON_DOB|PERSON_GENDER_CODE|PERSON_POSTCODE|DATE_AND_TIME|SITE_CODE|UNIQUE_ID|UNIQUE_ID_URI|ACTION_FLAG|PERFORMING_PROFESSIONAL_FORENAME|PERFORMING_PROFESSIONAL_SURNAME|PERFORMING_PROFESSIONAL_BODY_REG_CODE|PERFORMING_PROFESSIONAL_BODY_REG_URI|SDS_JOB_ROLE_NAME|RECORDED_DATE|PRIMARY_SOURCE|REPORT_ORIGIN|VACCINATION_PROCEDURE_CODE|VACCINATION_PROCEDURE_TERM|VACCINATION_SITUATION_CODE|VACCINATION_SITUATION_TERM|NOT_GIVEN|REASON_NOT_GIVEN_CODE|REASON_NOT_GIVEN_TERM|DOSE_SEQUENCE|VACCINE_PRODUCT_CODE|VACCINE_PRODUCT_TERM|VACCINE_MANUFACTURER|BATCH_NUMBER|EXPIRY_DATE|SITE_OF_VACCINATION_CODE|SITE_OF_VACCINATION_TERM|ROUTE_OF_VACCINATION_CODE|ROUTE_OF_VACCINATION_TERM|DOSE_AMOUNT|DOSE_UNIT_CODE|DOSE_UNIT_TERM|INDICATION_CODE|INDICATION_TERM|NHS_NUMBER_STATUS_INDICATOR_CODE|NHS_NUMBER_STATUS_INDICATOR_DESCRIPTION|SITE_CODE_TYPE_URI|LOCAL_PATIENT_ID|LOCAL_PATIENT_URI|CONSENT_FOR_TREATMENT_CODE|CONSENT_FOR_TREATMENT_DESCRIPTION



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?

The data will comprise of personal identifiable data and special category (health data) as defined within the UK GDPR and the Data Protection Act 2018. The data set has been defined by NHS England and PHE, and is the minimum required to complete a mass vaccination program. The term 'data' refers to both instances where information is processed where a vaccine is given and where a vaccine is declined.

The legal basis for the processing under Article 6 1. (e) is Public Task - in that the processing is being carried out in the public interest and in the exercise of official authority vested in the controller (an NHS Trust). The special category data requires a further consideration under Article 9 and this is 9.2 (h) processing is required for preventive or occupational medicine, (i)processing is necessary for reasons of public interest in the area of public health (the provision of and universal access to health care).

Further to this the collection and processing of data is covered by the Control of Patient Information Regulations 2002 and the corresponding COPI notice signed by the Secretary of State for Health and Social Care.

The data will be captured twice, as the vaccination is a two-part process with up to 12 weeks between doses, the geographical area is within the operational borders of the East of England Ambulance Service (although this may be widened to provide mutual aid or assistance to the wider NHS (the widest geographical area to be covered is the UK).

The processing of data will be maintained until the COPI notice is rescinded and then will be managed as part of the COPI de-escalation plan.

The number of data subjects involved is not clear at the present time and will alter if mutual aid is required, it is projected that it will not be less than 6000 data subjects.

All the processing of data under this project will occur within the UK and the data will reside within the UK or EEA.

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)?

The nature of the relationship between EEAST and the data subject will broadly follow three category, those directly employed by the Trust, those who directly/indirectly support the Trust to provide and maintain service provision, those who are employed by other NHS organisations for whom we are providing mutual aid.

A fourth category should also be considered in the light of the unpredictability of the pandemic, this is the general populace (both domestic and foreign). Although this is not currently planned it should be considered and noted.

Although individuals whose data is collected will have made an active choice to book an appointment, the data subject will need to provide medical consent for the vaccination to be given. The legal basis for the processing of the data has been previously given.

It would be expected that during a pandemic/mass vaccination scenario that this level of data would be collected by the NHS.

Currently it is not proposed that this system is used to collect details of those under the age of 18 (children), vulnerable groups including those shielding with long term health conditions etc will be included within the vaccination program.

There are no current concerns over processing this data, and no security flaws have been identified.

The total process comprises 3 systems that are already in daily use by the Trust and therefore are well established, as well as a cohort of expertise with each system.

The Trust has achieved standards met on the NHS Digital Data Security and Protection Toolkit.

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?
The purpose of the processing is to achieve the mass vaccination (to prevent the acquisition and spread of COVID 19) of those charged with providing an emergency ambulance service to the population of the East of England, approx. 5.5 million people. To protect staff and those working with the Trust from the risks to their health from acquiring the COVID 19 virus. The increase in immunity that will reduce or prevent the onward transmission of the virus by staff or those working closely with EEAST The reduction in mortality of staff, ancillary/support teams, patients, and the general population.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: 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?
Due to the limited time scales for the delivery of the solution it has not been possible to undertake a full and meaningful consultation. The Trust has brought together a group of staff together to implement the project that is broadly representative of the staff population as a whole.

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 the processing under Article 6 1. (e) is Public Task - in that the processing is being carried out in the public interest and in the exercise of official authority vested in the controller (an NHS Trust). The special category data requires a further consideration under Article 9 and this is 9.2 (h) processing is required for preventive or occupational medicine, (i) processing is necessary for reasons of public interest in the area of public health (the provision of and universal access to health care).

Further to this the collection and processing of data is covered by the Control of Patient Information Regulations 2002 and the corresponding COPI notice signed by the Secretary of State for health and Social Care.

The processing will achieve the objective and ensure that both the central NHS and the GP (the custodian of the Data Subjects Health Records) are informed of the vaccination status of the Data Subject. The system proposed will enable the Trust to provide mass vaccination to the target group.

To ensure data quality the Project Owner will commission a number of data quality audits, as well as spot checks. The data set has been defined by the NHS England and it is proposed that this is the maximum that the Trust will process.

The Trust Privacy Notice will be updated to provide the required information to individuals as well as sign posting them to appropriate individuals within the Trust who can provided greater detail. The Communications team are drawing up a comms plan that will include data security and information governance aspects.

EEAST holds NHS Standard Contracts with those who provide the various systems, and will be the Data Controller for the proposed solution, as well as being a data processor for parts thereof.

The Trust will ensure that all data subjects are able to exercise the rights provided to them through the Data Protection Act and the UK GDPR.

Any data being processed as part of this solution will be maintained within the UK or EEA and therefore fall under the GDPR, UK GDPR and Data Protection Act 2018, the supervisory body will be the Information Commissioners Office (ICO)

Step 5: Identify and assess risks

Risk	**Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. See the Risk Matrix in Appendix D.	**Likelihood of adverse effect**	**Severity of adverse effect**	**Overall risk rating** Overall risk = Likelihood multiplied by Severity
		5, 4, 3, 2, 1	**5, 4, 3, 2, 1**	
1a: Loss of Data	Data loss through the corruption of data or the physical loss of a database | NHSE and PHE will not know who has been vaccinated | Individual GPs will not know if their patient has been vaccinated	2	1	3
2a: Misuse of data	Breach of any of the systems by external agents, or rogue internal agents leading to data theft	2	3	6
3a: Integrity/accuracy of data	Inaccurate reporting to NHSE, PHE, inaccurate supply of relevant information to patient GP | the inability to trace an individual if a recall is required	3	3	9
4a: Unauthorised access/disclosure	Inappropriate access to, extraction of information a subsequent disclosure			
	a) An individuals record, inappropriate pressure brought to bear on the individual to act in a particular way	2	4	8
	b) The release of aggregated information leading to reputational damage	3	4	12

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 control the risk.** Include solutions for reducing or controlling the risks listed above.	**Effect on risk**	**Residual risk** This score should match the Severity scoring above	**Risk control score** Risk control score = Effect multiplied by Residual
1a: Loss of Data	Using established systems from established providers that include back up solutions and disaster recovery plans | EEAST Business Continuity Plans	1	1	1
2a: Misuse of data	All systems employ access controls , which include password allowing data to be segregated ensuring that users only see the data they need to complete the required task | Trust Policies and Procedures for the and profile settings Breach of any of the systems by external agents, or rogue internal agents leading to data theft	2	3	6
3a: Integrity/accuracy of data	Inaccurate reporting to NHSE, PHE, will be reduced by the direct entry of data onto the NIV system and monitored by audit and spot checks | reconciliation using the national spine to reconcile data subject with the correct GP practice	2	3	6
4a: Unauthorised access/disclosure	Inappropriate access to, extraction of information a subsequent disclosure			
	a) Minimal data storage and access to individual level data, appropriate use of pseudonymisation and encryption | strong policies and procedures	2	4	8
	b) Appropriate access controls to raw and aggregated data | strong policies and procedures	2	4	8

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Emma Sears, Legal Services Manager (DPO) 11 January 2021	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Emma Sears, Legal Services Manager (DPO) 11 January 2021	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Emma Sears, Legal Services Manager (DPO) 11 January 2021	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Discussion with GDPR Implementation Lead around aspects of the DPIA that required clarification for my understanding. Noted use of Article 9 (h) and (i). Discussed the risks and that the residual risk for 4a is still high at 8, all relevant and possible actions are being taken. Approved.		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA
DPIA Valid Until Date (VDU):		We recommend a minimum of 3 years after approval date, unless there are significant changes to the processing or risks.