Submitting controller details

Name of controller	North Staffordshire Combined Healthcare
Subject/title of My OH Portal	My OH Portal
Name of controller contact	Alexa Lloyd, Senior HR Advisor
Information Asset Owner	Shajeda Ahmed, Director of Workforce, OD & Inclusion
Information Asset Administrator	Kerry Smith, Associate Director of Workforce

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.
Main System Development Team Prevent are developing a new Occupational Health database system to manage customer Occupational Health Medical records, book appointments, manage diaries and record activity. The new database will help our administration and clinical teams manage all aspects of the Occupational Health Service. The system will be called MyOH and will replace the current system referred to as eOPAS. The migration to the new system is expected to go live on 14th October 2020. Because of the nature and volume of information being processed it is necessary to ensure that the system is designed and developed in such a way that keeps the information secure. Both systems have an online "portal" that can be accessed by Managers, HR, Recruitment and employees, there are access control procedures in place to restrict the type of access each user has. **Migration of existing Data from eOPAS to MyOH** The project will also involve transfer of data from the eOPAS system to the MyOH system for each customer and this documented has now been updated to include the data flows and risks associated with this are also mentioned in this document.

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?
Personal Information stored in the system is used for the following purposes: • To arrange and book appointments with the Occupational Health Team. • To contact people if we need to move or change an appointment. • To contact people to undertake a telephone or online video appointment. • To verify that we are speaking to the correct person, if you phone us to query your health records. • To send text message and email reminders about appointments Depending on the nature of an employee's job Health Records may be used for the following purposes: • To determine fitness to work. • To assess if the need for any adjustments or support in the workplace because of a health condition. • To establish if any risks in the workplace may have an adverse effect on your health. • To provide information about your fitness to work back to your employer. Team Prevent will also routinely carry out analysis of Health Data that they have recorded about a customer's workforce in order to identify key trends and patterns in activity and health. This data is fully anonymised which means it is impossible to identify any individual from the information. Data Migration from the current eOPAS system to the MyOH system is being managed used a separate standalone data migration tool. The tool has been developed interdependently from the MyOH system to avoid the risk or possibility of it being used by an unauthorised user. Appropriate physical and electronic controls are in place to secure access to the tool and to ensure access is restricted to authorised users only. The tool facilities a direct TLS

secure link between the Team Prevent SQL Database housing the eOPAS system and the new MyOH database to enable data to be transferred directly from one system to another.

Certain data is migrated using the following steps

- Downloaded from eOPAS
- Mapping
- Cleansing old data

Data transferred in the above way includes *Customer Users* and *Due Tasks*. This is so that the correct access rights can be applied to the customer users and so that “Due tasks” can be assigned to different cases within the new system and ONLY relevant and up to date new tasks are created in the new system.

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 scope of the processing and data collection is highlighted below and is collected from employees from NCHT for the purposes of offering support and essential monitoring (e.g. vaccine/health surveillance) at work:

Forename, Surname, DOB, Job Title, personal home number, mobile number, personal email address, work email address

Health records – Special Category data

	Type of Data	Data Flow / Direction including Departments	Proposed method of data flow	Type of data being accessed or flowing	Storage of the data
1	**Referrals made by Managers or OH to Team Prevent**	Manager or HR TO Team Prevent	Via online portal accessed by Manager or HR (data will not leave COSMOS DB)	Personal information including, name, DOB, address, contact phone number, email address. Special category data - Health Information	MyOH system on COSMOS DB
2	**Management Referral reports back to Managers and HR**	Occupational Health team TO HR	Via online portal accessed by Manager or HR (data will not leave COSMOS DB)	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
3	**Pre-placement questionnaires sent to employee by Recruitment team to complete**	Recruitment team TO Candidate/Employee	Via online customer portal TO online employee portal. (data will not leave COSMOS DB)	Personal information including, name, DOB, address	MyOH system on COSMOS DB
4	**Completed Pre-placement questionnaire sent from candidate back to Team Prevent**	Candidate TO Occupational Health Team	Via online portal accessed by Manager or HR (data will not leave COSMOS DB)	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
5	**Pre-placement Certificates back to Recruitment Team**	Occupational Health team TO Recruitment	Via online portal accessed by Manager or HR (data will not leave COSMOS DB)	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
6	**Completed Health Surveillance questionnaires sent from employees back to Team Prevent**	Customer Employee TO Occupational Health Team	Via online portal accessed by Manager or HR (data will not leave COSMOS DB)	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
7	**Appointment Reminders and notifications**	Occupational Health Team TO Customer employee	Via email, text message and online portal	*Appointment details*	*MyOH system on COSMOS DB, mail server*

8	**Vaccination Records**	Clinical Team TO MyOH System	Vaccination records are created in the system and point of vaccination by direct data input	Special category data - Health Information	MyOH system on COSMOS DB
9	**Information relating to Blood Tests**	Laboratory test results to MyOH System	Records from the laboratory are inputted into the MyOH system and any documents scanned and attached to employee health record	Special category data - Health Information	MyOH system on COSMOS DB
10	**Requests for GP Letters**	Occupational Health Team TO employee's GP/Specialist or treating specialist	Post or secure encrypted email. Consent obtained from employee and then information sent to GP/Specialist	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
11	**Medical letters received back from GP's**	Employee's GP or treating specialist TO Occupational Health Team	Information is sent via Post or email	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
12	**Analysis of data for MI purposes**	From OH System to Data Analytic tool	Via secure connection directly to COSMOS DB	Anonymised Health Information	MyOH system on COSMOS DB
13	**Subject Access Requests**	Occupational Health team TO 3rd Party or Data Subject	Data is downloaded from system to send to 3rd Party or Data Subject	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB
14	**Transfer of data to new OH Provider**	Occupational Health team TO New OH Provider	Data is downloaded from system to send to 3rd Party or Data Subject	Personal information including, name, DOB, address. Special category data - Health Information	MyOH system on COSMOS DB

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 system security architecture described in the technical section has been deliberately chosen to ensure the data remains secure and privacy between individual records and customers is maintained at all times. Team Prevent are working with a specialist development partner in order to ensure that the correct technical and project skills are being used at all times. During Development each new feature or functionality of the system will be designed using an experienced Business Analyst who will work in consultation with the representatives from Team Prevent to Individual Written "user stories" all identify privacy risks and then go on to describe how this risks will be managed within that particular story or feature. Consultation on these "user stories" including privacy risks is between the Business Analyst and Team Prevent IT Director and Team Prevent Operations Director. QAT and UAT testing always incorporates privacy testing to ensure data remains viewable by the correct people. Where there are high levels of privacy risk identified further consultation will take place with the Senior Developer or the Chief Technical Officer within the Development partner. Extensive consultation is already taking place between the CTO and Senior Development and IT Director on the correct approach to data migration. Controlling all data privacy issues during data migration remains of upmost importance and is the primary reason the technical solution described below has been chosen.

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 current system is clunky and time consuming for managers HR and employees to use. The new system will provide more visibility of your Occupational Health record giving employees, managers and HR access online to their Case History that will include appointment information, immunisation and blood test history, occupational health reports and referrals that have been made by the manager. This will also support the HR team to advice managers on the most appropriate support available in line with trust policy.

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 developments in Team Prevent IT systems as they are the Trust OH provider there is the requirement to migrate across to MyOH Portal as part of the contract. This is a requirement of all NHS Trusts that have an OH contract with Team Prevent. Team Prevent are working with a specialist development partner in order to ensure that the correct technical and project skills are being used at all times. During Development each new feature or functionality of the system will be designed using an experienced Business Analyst who will work in consultation with the representatives from Team Prevent to Individual Written "user stories" all identify privacy risks and then go on to describe how this risks will be managed within that particular story or feature. Consultation on these "user stories" including privacy risks is between the Business Analyst and Team Prevent IT Director and Team Prevent Operations Director. QAT and UAT testing always incorporates privacy testing to ensure data remains viewable by the correct people. Where there are high levels of privacy risk identified further consultation

will take place with the Senior Developer or the Chief Technical Officer within the Development partner.

Data Migration note added 27th May: Extensive consultation is already taking place between the CTO and Senior Development and IT Director on the correct approach to data migration. Controlling all data privacy issues during data migration remains of upmost importance and is the primary reason the technical solution described below has been chosen.

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?

All data is processed in UK Microsoft Azure data centres *(updated 2nd September 2020 following migration from EU data centre to UK data centre of MyOH)*

Article 6 item (f) legitimate interests, and under Article 9(2) item (h) for the purposes of occupational medicine

Step 5: Identify and assess risks

Step three: identify the privacy and related risks Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Appendix C can be used to help you identify the DPA related compliance risks.		
Number	Privacy Issue	Description of the Risks

1)	Back end database is not secure enough and is vulnerable to data attacks	Data accessed maliciously by a 3rd party could lead to a major data loss and breach of sensitive personal information into the public domain
2)	Back end database is not being run on up to date software making it vulnerable to data attacks	Data accessed maliciously by a 3rd party could lead to a major data loss and breach of sensitive personal information into the public domain
3)	Access to main Team Prevent web application and database is not sufficiently controlled	Secure access is required into the main Team Prevent database that ensures only authorised Team Prevent personnel who have been trained can access data for multiple customers. Risk is customers, other 3rd parties or other users in Team Prevent with insufficient access rights can access the system and see data they are not supposed to see. Could leave to major data loss
4)	Access to main customer web applications is not sufficiently controlled	Secure access is required into the main Team Prevent database that ensures only authorised Team Prevent personnel who have been trained can access data for multiple customers. Risk is customers, other 3rd parties or other users in Team Prevent with insufficient access rights can access the system and see data they are not supposed to see. Could leave to major data loss
5)	Customer data is not segregated properly in the system	Customers can see data relating to other customers. Would be classified as a major data loss
6)	Data entry into the system is poor leading to poor inaccurate records being held	Failing to hold up to date and accurate records on staff could lead to a failure to contact the correct person or to releasing data and information to the wrong person. This would be a data loss or breach/incident
7)	Data being submitted from the customer to the OH Team is lost or intercepted	Referrals and questionnaires being sent from the customer to the OH Team can be lost in transit if postal services are used or can be intercepted if mail is not secure
8)	Data being sent from the OH Team to the customer / employee is lost or intercepted	Reports and other information being sent from Team Prevent to the customer can be lost in transit if postal services are used or can be intercepted if mail is not secure
9)	Data Subjects are not aware of how data is being processed	Data Subjects must be informed about processing and Team Prevent must be transparent about what is happening and why
10)	Data is stored on local devices which may not be secure when accessed by customer or employee through “cache” or via use of native applications	Data on a local device could easily be lost or stolen. Unencrypted or poorly encrypted devices may be easy for someone else to access and view the data, leading to a data loss
11)	Customer users can see data they are not supposed to see when accessing the system	Users should only be able to see data they are supposed to see. IF they can see data relating to other employees or staff when they do not have authority to do so then this would be considered a data incident/breach
Migration of data risks added below		
1)	Data is not secure during transit from eOPAS to MyOH	Data must be transferred using a secure TLS encrypted connection or there is a risk of interception and data loss

2)	Data transferred from eOPAS to MyOH is incorrect	If data is not "mapped" correctly to appropriate fields OR appropriate employee records then data could be imported into MyOH that is incorrect
3)	Data uploaded via csv file is not correct	If data is not "mapped" correctly to appropriate fields OR appropriate employee records then data could be imported into MyOH that is incorrect As this data is moving from a manual file into MyOH and NOT directly from SQL to COSMOS there is an increased risk of error
4)	Historical data in eOPAS is not deleted correctly	eOPAS system has a "data deletion" tool that can be used to delete all data from the system. As data backup are incremental then overtime backup's will also be deleted leaving no trace of the data
5)	Data Migration tool is used incorrectly or inappropriately	If used by the wrong person or used in error then data can migrate incorrectly or at the wrong time which could lead to a data loss or breach of data
6)	Customer user accounts are Linked to incorrect cases	Customer's users see cases that they are not authorised to see post migration. Leading to data breaches because reports and medical information would be available for the wrong people to see
7)	Key Customers are not aware of data migration project taking place	Duty of care and responsibility to inform about how data is processed is

Step 6: Identify measures to reduce risk

Step four: Identify privacy solution
Describe the actions you could take to reduce the risks, and any future steps which would be necessary (E.g. the production of new guidance or future security testing for systems).

Number	Risk	Solution(s)	Result: is the risk eliminated, reduced, or accepted?
1)	Back end database is not secure enough and is vulnerable to data attacks	Suitable modern cloud based database technology to be used. Recognised secure provider (Microsoft) being utilised. System architecture being put in place by recognised development team	Minimised as far as possible, residual risk is acceptable
2)	Back end database is not being run on up to date software making it vulnerable to data attacks	Cloud based systems being used with automatic patching processes in place. Systems are therefore always kept up to date and patching applied every 2 weeks	Eliminated
3)	Access to main Team Prevent web application and database is not sufficiently controlled	Access will be designed to it is linked to TP Active directory controlled by MS 0365 tenant, this include strong password enforcement and MFA for all users	Minimised as far as possible, residual risk is acceptable
4)	Access to main customer web applications is not sufficiently controlled	Microsoft B2C solution to be used for access. Access controls will also need to be built into the system to allow user access control for customer users (HR, Recruitment, Super User etc.). MFA to be considered for future access	Minimised as far as possible, residual risk is acceptable

5)	Customer data is not segregated properly in the system	Core system architecture most deploy suitable sharing of the customer data at a high level. Key design consideration during first few development sprints	Eliminated
6)	Data entry into the system is poor leading to poor inaccurate records being held	Mandatory fields and drop down menus to be used at all available opportunities. Other validation techniques on date and time fields and other numerical fields to always be considered in the system design	Minimised as far as possible, residual risk is acceptable
7)	Data being submitted from the customer to the OH Team is lost or intercepted	New system is to be designed so ALL information stays within the system/database and there is no requirement for the customer to submit information by post, email or other form of communication. Online forms to be developed with ability to attach documents	Eliminated
8)	Data being sent from the OH Team to the customer / employee is lost or intercepted	New system is to be designed so ALL information stays within the system/database and there is no requirement for the customer to submit information by post, email or other form of communication. Online forms to be developed with ability to attach documents	Eliminated
9)	Data Subjects are not aware of how data is being processed	Data Privacy Statement on Team Prevent website will be kept up to date to reflect use of the new system Privacy statement questions to be incorporated within the clinical notes, at the start of referral forms and at the start of all questionnaires Access to privacy statement to be provided in manager and employee portals	Minimised as far as possible, residual risk is acceptable
10)	Data is stored on local devices which may not be secure when accessed by customer or employee through “cache” or via use of native applications	Webapps will be deployed instead of a native app on a user’s device. This means all data stays “on the database” and is not cached or stored local in anyway	Eliminated
11)	Customer users can see data they are not supposed to see when accessing the system	Access controls to be introduced by HR, Recruitment and Manager user Org structures will not be used to control access to information, the principle of the manager who makes the referral can see the data is adopted instead	Minimised as far as possible, residual risk is acceptable
Migration of data risks added below			
1)	Data is not secure during transit from eOPAS to MyOH	Migration tool uses secure TLS 2.0 encrypted connection to ensure data is secure in transit. Complex 25 character authentication key used for access to COSMOSDB. Access to Team Prevent SQL database controlled via Active	Minimised as far as possible, residual risk is acceptable

		Director authentication to limited number of users with access privileges to the DB	
2)	Data transferred from eOPAS to MyOH is incorrect	1 unique keys and 2 other keys to be used for transfer of all records. Personal reference number (unique key), DOB and Customer for each set of data MUST Match for data to be placed on the employee record. Enhanced QAT and UAT testing before live release of data migration tool will take place to verify tool is working correctly. Each customer will have a "test data transfer" the week before "Live transfer"	Eliminated
3)	Data uploaded via csv file is not correct	1 unique keys and 2 other keys to be used for transfer of all records. Personal reference number (unique key), DOB and Customer for each set of data MUST Match for data to be placed on the employee record. Enhanced QAT and UAT testing before live release of data migration tool will take place to verify tool is working correctly. Written SOP in place for creating of csv file that incorporates second person check	Minimised as far as possible, residual risk is acceptable
4)	Historical data in eOPAS is not deleted correctly	Deletion SOP has been written Software vendor has provided an appropriate deletion tool that ensure all data is removed and digital footprint of the data is completely deleted	Eliminated
5)	Data Migration tool is used incorrectly or inappropriately	Stand-alone Data Migration tool will be developed that is not linked to the main application. Tool to have appropriate physical and electronic security measures in place to restrict access and use	Minimised as far as possible, residual risk is acceptable
6)	Customer user accounts are Linked to incorrect cases	1 unique keys and 2 other keys to be used for transfer of all records. Personal reference number (unique key), DOB and Customer for each set of data MUST Match for data to be placed on the employee record. Enhanced QAT and UAT testing before live release of data migration tool will take place to verify tool is working correctly. Written SOP in place for creating of csv file that incorporates second person and third person check of the data prior to upload.	Minimised as far as possible, residual risk is acceptable

		Only "recent cases" to be migrated to reduce risk of historical cases that are now being managed by	
7)	Key Customers are not aware of data migration project taking place	Team Prevent Privacy Statement to be kept up to date Communications strategy agreed with the trust to make people are aware of the transfer to a new system	Minimised as far as possible, residual risk is acceptable

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Alexa Lloyd, Snr HR Advisor drafted DPIA & Laura Ross, Workforce Business Partner 8th October 2020	All risks have been assessed and mitigations outlined. Where risks remain these have been mminimised as far as possible and residual risk is considered acceptable.
Residual risks approved by:	Kerry Smith, Associate Director of Workforce 8th October 2020	Residual risk consulted with Alexa Lloyd and Daniel Crick Deputy Chief Information Officer on 29th September 2020
DPO advice provided:	Lorraine Forrester Health Records & Information Governance Manager Health Records Department 28th September 2020 This DPIA has identified all the risks involved and added actions to be taken to reduce or mitigate them.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Just a number of track changes made.		

DPO advice accepted or overruled by:	**Accepted** Lorraine Forrester Health Records & Information Governance Manager Health Records Department	N/A
Comments: N/A		
Consultation responses reviewed by:	Alexa Lloyd, Snr HR Advisor Laura Ross, Workforce Business Partner Kerry Smith, Associate Director of Workforce Daniel Crick Deputy Chief Information Officer Lorraine Forrester Health Records & Information Governance Manager Health Records Department	N/A
Comments: N/A		
This DPIA will be kept under review by:	This will be reviewed in line with OH contractual changes. Kerry Smith, Associate Director of Workforce Delegated responsibility to appropriate lead.	The DPO should also review ongoing compliance with DPIA