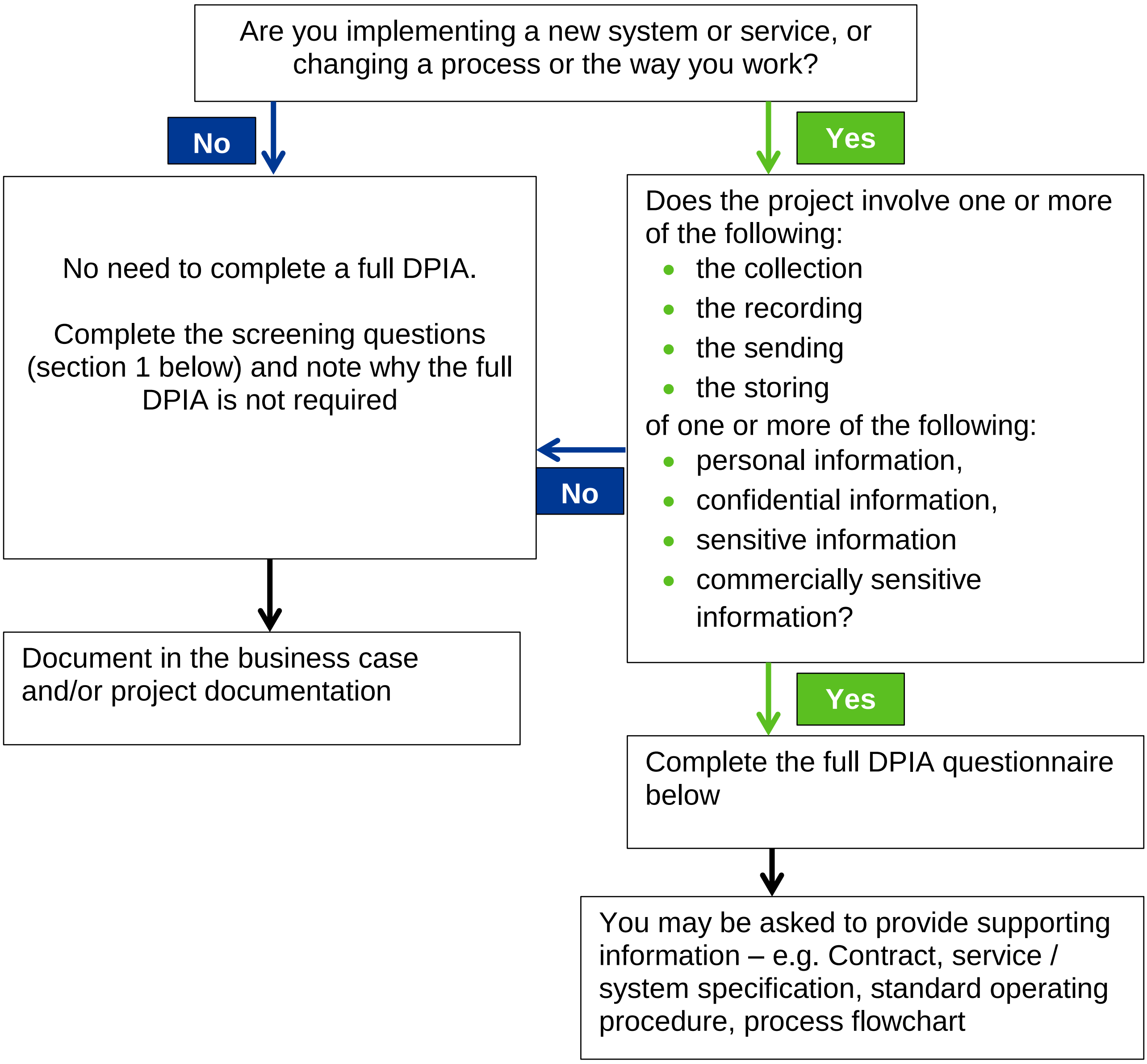
Data protection impact assessment (DPIA) template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

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.

Use the below flowchart as a guide if you are unsure whether or not to complete this template:

Do I need to complete a DPIA?



Are you implementing a new system or service, or changing a process or the way you work?

No

No need to complete a full DPIA.

Complete the screening questions (section 1 below) and note why the full DPIA is not required

Document in the business case and/or project documentation

Yes

Does the project involve one or more of the following:

- the collection
- the recording
- the sending
- the storing

of one or more of the following:

- personal information,
- confidential information,
- sensitive information
- commercially sensitive information?

No

Yes

Complete the full DPIA questionnaire below

You may be asked to provide supporting information – e.g. Contract, service / system specification, standard operating procedure, process flowchart

Details of DPIA

Name of project	MCH Data Warehouse
Synopsis of project	Installation of data warehouse at Custodian data centre, Maidstone.
Name and job title of person completing this DPIA	[redacted], AD Business Intelligence
Date	05/09/2019

Step 1: Screening questions

Screening question	Response (Yes/No)	Rationale
Will the project involve the collection of new information about data subjects? (e.g. patients, staff)	No	This project relates to the processing of existing data.
Will information about individuals be disclosed to organisations or people who have not previously had routine access to that information?	Yes	blueFish Intelligence Ltd will be granted access to the data warehouse
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	
Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	No	
Is the information about individuals of a sensitive nature, likely to raise privacy concerns or expectations? (e.g. health records, criminal records)	Yes	Health records and staff data

If you have answered “Yes” to any of the above please continue to Step 2 below

If you have answered “No” to all of the above questions then send this to the IG team medch.dataprotection@nhs.net. You do **not** need to complete the rest of this form

Step 2: Identify the project aims / objectives

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.
As part of its transformation strategy, MCH has committed to improving its capacity and competency in respect of producing performance reports and processing data into business intelligence. This project is also being undertaken as a mitigating action against two key corporate risks for MCH (Datix ID numbers 1948 and 2099). This project has two main components: 1) Installation and set-up of a new data warehouse at the Custodian data centre in Maidstone (by ICOM Telecommunications) 2) Granting access to the data warehouse to blueFish Intelligence Ltd so that it can provide business intelligence services to MCH. This will include construction of tables and cubes for processing data that will be imported from clinical and non-clinical systems. The need for a DPIA is based on the fact that blueFish Intelligence Ltd (bFI) will be a data processor on behalf of MCH (the data controller). Although bFI will not store any data, they will require access to MCH's data in order to implement software and processes that will help automate reporting for MCH.

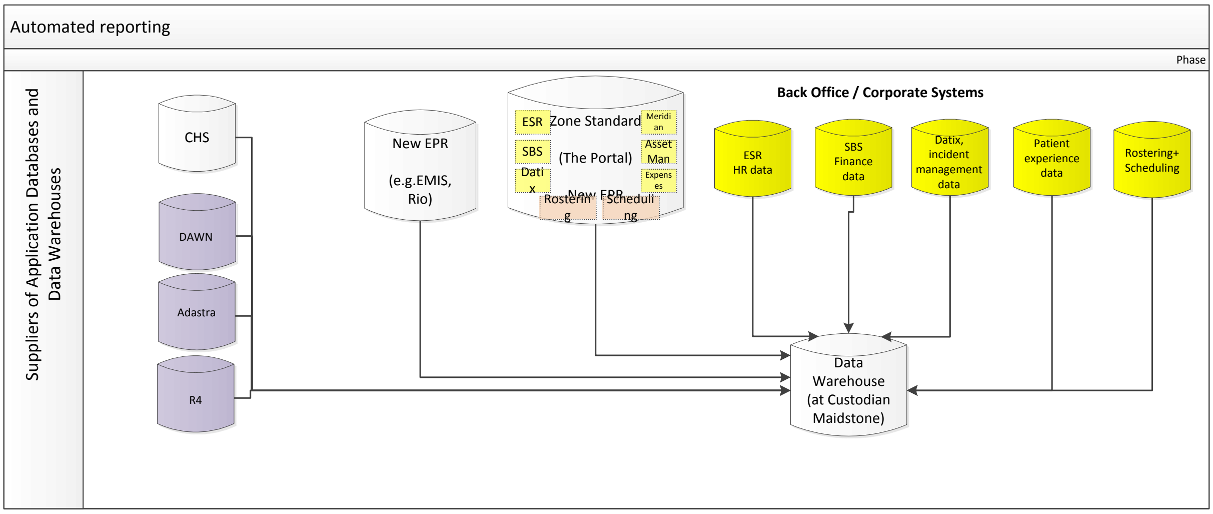
Step 3: Describe the processing

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?

MCH will provide bFI access via secure login credentials to the data warehouse at Custodian. Data will not be copied and bFI will not store the data nor will it share data with any third parties.

Personal data including special category health data that has been recorded electronically by MCH staff across several different IT applications will be extracted and copied data warehouse based at Custodian, Maidstone.

The diagram below is an outline schematic showing the core applications from which data will be extracted and loaded into the data warehouse.



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 nature of the data stored is as follows and includes special category healthcare data:

Patients/Service Users – service identifier, name, Address, DOB, NHS no, registered GP, referrer, sensitive data ethnicity, physical/mental health condition (clinical notes), consultation outcomes caller's details (in case someone calling on behalf of the patient), appointment dates, times and locations.

Staff/employees - Name, Address, ethnicity, employment details, skills, record number and record of background checks such as DBS can be uploaded.

Data collected relates to services that run out of hours as well as in hours covering 24 hours a day, 7 days a week, and including bank holidays.

Data is retained in line with national guidance for healthcare data which is between 5 to 10 years for adults and up to the age of 25 for some childrens records. Data will be erased in line with national guidance.

Geographical area is Kent & Medway and those temporarily visiting the area.

Approximate number of patients affected per annum will be 150,000 to 200,000.

The main patient population is Medway and Swale with a population of 433,869:

Medway CCG registered population (Jan 2015) 291,452

Swale CCG registered population (Jan 2015) 142,417

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 MCHs relationship with the data subjects is as employer and as a healthcare provider to patients. Information is collected by healthcare professionals and administrators all of which are required to attend annual mandatory IG training. Discussions about the use of data are held between healthcare professionals (staff) and patients and the patients have an option to opt out.

Our patients are expecting us to use their data in this way.

We will include data relating to children and other vulnerable groups.

There are no prior concerns over this type of processing.

No it is not novel in any way.

Other healthcare organisations across Kent & Medway and indeed nationally are already using this type of technology.

No public concerns have been reported.

Data will be stored at the Custodian data centre in Maidstone in the UK and will not be sent overseas or outside of the UK. The Custodian data centre has also been chosen as the preferred data warehouse location by the majority of other major healthcare providers across Kent & Medway including Maidstone and Tonbridge Wells Trust, Medway Foundation Trust, Kent Community Health Foundation Trust, East Kent Hospitals Foundation Trust.

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?

Currently MCH is struggling to meet its contracted data and reporting obligations. The existing human resource spends the vast majority of its time processing data manually. Technology exists which could help automate tasks, reduce the scope for data errors and help identify data quality issues.

The aims of the project are to resolve the issues highlighted above by creating an infrastructure that will:

- reduce the time it takes to produce reports that MCH is contracted to provide
- free up time and capacity to analyse performance across a wide range of services across the business
- support services maintain or improve quality of services for patients (including analysis that supports the redesign of pathways)
- provide data and insights that will support decision-making in respect of retention and award of contracts

Step 4: 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?

Meetings with operation managers and processors held in order to process map the way each service operates.

Panel of 6 members:

SIRO: [redacted]

DPO: [redacted]

Caldicott Guardian: [redacted]

IT Controller: [redacted]

Senior User: [redacted]

Technical Lead: [redacted]

The core IT applications from which the data will be extracted and processed are already in place. The IT applications currently include: CHS (Advanced), ESR (Employment staff record), Adastra (OOH clinical system). This project only grants bFI personnel (circa 5 individuals) additional access to the data for the purposes of data manipulation. Data is not copied or stored by bFI and therefore we have deemed consulting with patients is not necessary.

Step 5: 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 lawful basis for processing patient health records will be GDPR Article 6 (E) Public Task (delivery of publicly funded services) and the legal bases for processing special category information will be GDPR Article 9 (H) Delivery of healthcare. MCH is the data controller and bFI is the data processor. The lawful basis for processing staff records will be Article 6(b) contract (we have an employment contract with individuals) and for processing special category staff information will be Article 9 (b) obligations of employment and social security.

We have considered reduced information or including additional information and have concluded that this strikes the right balance of risk and benefit in the interests of the subject.

It is not envisaged that the information would be used for other purposes. Supplier contracts prohibit the use of the information for other purposes. Internal rules prevent the use of the information for other purposes with the exception of statistical monitoring and approved research in line with national guidelines.

There are no implications for Responding to SARs (right to access) this process will remain the same; if blueFish receive a SAR then it is in our data sharing agreement that it will be forwarded to us as Data Controllers within 1 working day.

MCH will control access to the data warehouse by applying role based access that will mirror the permission that staff have to the core applications from which the data will be extracted. This will mean that the default access for staff will be to view aggregated data but staff that have a role which requires access to the patient level data in order to fulfill their duties will have permission to ‘drill-down’ to that level of detail.

Our patients expect us to use their data in this way.

Use of data warehousing technology and processes will mean data quality reports and checks will be introduced to address and improve existing data quality issues.

Security controls include:

- [redacted]

The contracted primary and secondary (back up) data centres are both located in the UK and data will not be transferred out of the sites.

Step 6: Identify and assess risks

Consequence ⇨ Likelihood ⇩	1 Negligible	2 Low	3 Medium	4 High	5 Extreme
1 Rare	L1	L2	L3	M4	M5
2 Unlikely	L2	L4	M6	M8	S10
3 Possible	L3	M6	M9	S12	H15
4 Likely	L4	M8	S12	H16	H20
5 Almost Certain	M5	M10	S15	H20	H25

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

Record all risks here with proposed controls that have been identified. Click here for examples of risks & controls.

No.	**Summary of risk**	Likelihood of harm	Consequence	Overall risk score
1	[redacted]	1	4	M4
2	[redacted]	3	4	S12
3	[redacted]	2	4	M8

4	[redacted]	2	4	M8
5	[redacted]	1	4	M4
6	[redacted]	2	4	M8
7	[redacted]	2	4	M8
8	[redacted]	2	4	M8

Step 7: Action plan to reduce risk(s)

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6. If you have a project plan then the below actions should be reflected in it. Any risks should be added to the service/project risk register.

Risk no.	Actions required to implement proposed controls (from step 6)	Target residual/ risk score	Action owner and target date	Review date	[redacted]
1	[redacted]	4	[redacted] - ongoing	30/04/2020	
2	[redacted]	4	[redacted] – 30/09/19 [redacted] – 30/09/19	30/09/2019	

3	[redacted]	4	[redacted]- ongoing	30/04/2020	
4	[redacted]	4	[redacted]) – 30/09/19 [redacted]) – 30/09/19	30/09/2019	
5	[redacted]	4	[redacted]– to review at each quarterly performance meeting	30/04/2020	

6	[redacted]	4	[redacted]- 30/10/19	30/10/2019	
7	[redacted]	4	[redacted] - 30/10/19	30/10/2019	
8	[redacted]	M4	[redacted] – 30/9/19	30/9/2019	

Step 8: Sign off and record outcomes

Signed by project lead (person completing the DPIA)

Name: [redacted]

Position: Associate Director Business Intelligence

Signed: [redacted]

Date: 18-9-2019

Now send the completed DPIA form to medch.dataprotection@nhs.net to be reviewed by the DPIA panel.

DPIA panel (Information governance team)

DPO consulted	☒
SIRO consulted	☒
Caldicott Guardian consulted	☐

Comments and recommendations:

Nil
Processing can commence.

Final sign off

Name: [redacted]

Position: Director of Finance and Resources / Senior Information Risk Owner (SIRO)

Signed: [redacted]

Date: 19/09/19