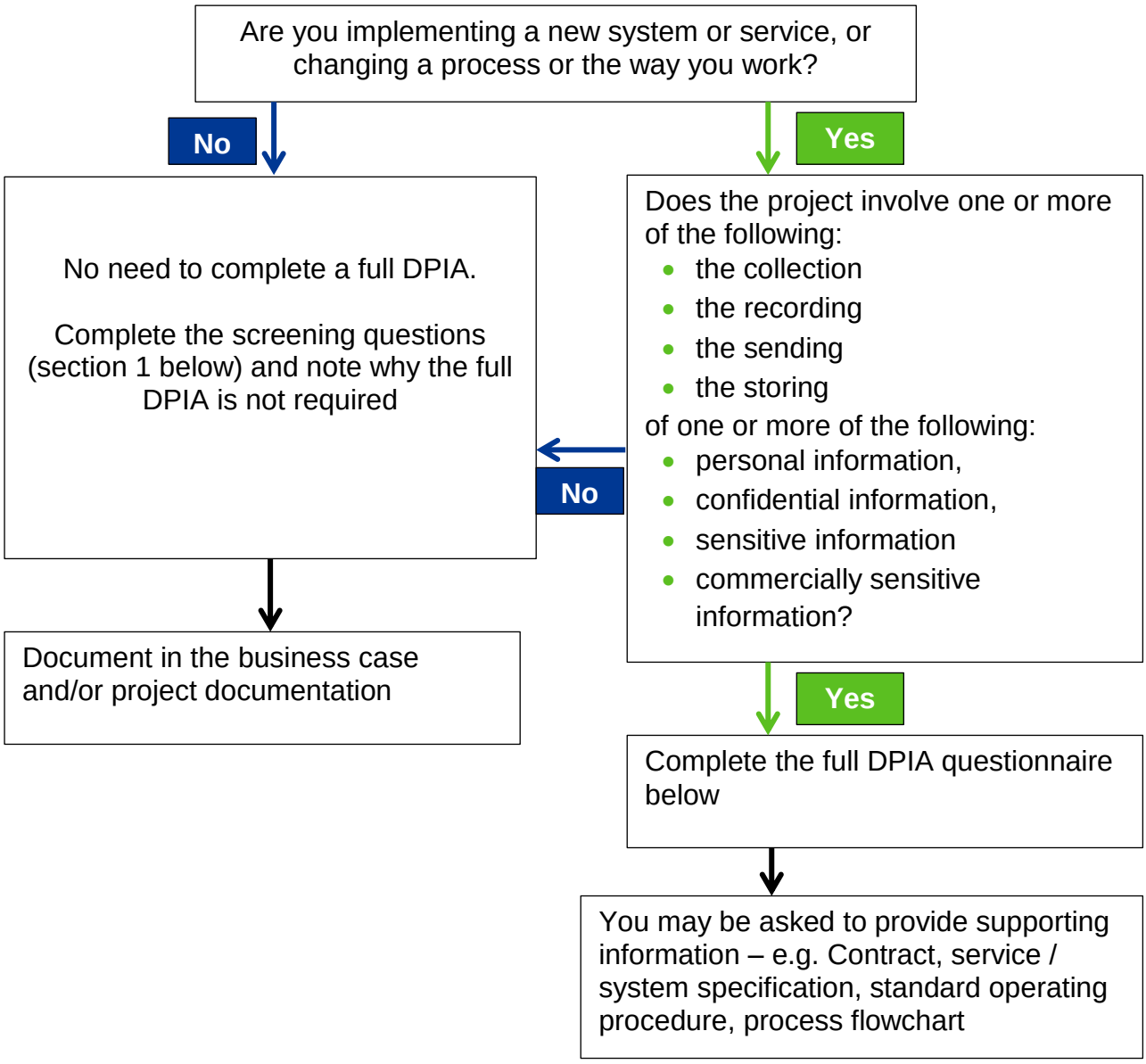
Data protection impact assessment (DPIA) template

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?



Details of DPIA

Name of project	Synertec Hybrid Mailing Solution
Synopsis of project	To implement a hybrid mailing solution to streamline the sending of patient letters by post and email, and alleviate the pressure on admin staff to carry out this manual task
Name and job title of person completing this DPIA	[redacted]
Date	27th November 2018

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	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to that information?	Yes	We will be outsourcing the emailing/posting of patient letters to Synertec, who have not had access before
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes	Outsourcing emailing/posting of patient letters to an external organisation which has before been managed in house
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 - appointment letters, discharge letters, did not attend letters

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.
The project aim is to implement a Hybrid mailing solution across MCH replacing the current manual process. Current process for mailing letters to patients is time consuming and has a high cost. Currently, admin staff will print the letter out, assign priority, envelope letter, stamp letter and post it. This process takes approximately 2 minutes per letter, while with a hybrid mailing service our admin staff will spend approximately 10 seconds per letter. There will be a cash releasing benefit of about £30,000 per annum from postage and printing cost and it will save our staff 8000 working hours per year. There are reports that a hybrid mailing solution reduces DNAs and also reduces the IG risk of an IG incident occurring with the manual process, eg. a member of staff adding two different patient's letters in one envelope; or sending an email to the wrong recipient. A DPIA needs to be completed as we will process personal data without providing a privacy notice directly to the individual and because we are going to process special category data or criminal offence data on a large scale.

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?
Patient letters will be printed to a remote printer by our staff. Synertec will print these letters out by using Prism software suite, which automatically identifies the patient and GPs addresses (whatever is on the letter). The software will then either put the letter into an envelope to be posted, or it will email the letter to the patient/GP if the email address is on the patient letter or within the Prism database. The emails will be sent from an NHS.net account: medch.prism@nhs.net When emailed these will be sent as a password protected PDF document. GP letters will be emailed without encryption as this poses an increased burden for GP surgeries, and the letters will be sent from and to both NHSmail accounts. When emailing patient letters, Synertec will send out one email containing the attached letter, along with the information on how they can unlock the password protection. An example of the email is below: *"Please find attached a letter from Medway Community Healthcare. To ensure the letter is kept as secure as possible, a password is needed to open the letter.* *The password to open your letter is the first letter of your First Name followed by the first letter of your Surname and then your date of birth. For example: if your name is John Smith*

and your date of birth is 24/08/1984 your password would be JS24081984. Please remember to use capital letters"

The information that Synertec will be able to access is patient demographics (name, address, NHS number) and details relating to an appointment (date, time, location, clinician seeing) and consultation outcomes (eg. a discharge letter sent to a GP).

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 items that will be extracted are:

- Service Identifier
- Name of Patient
- Patient Address (as per Patient Demographic Service)
- NHS number
- Date of Birth
- Registered GP
- Consultation outcomes
- Next appointment(s) date(s).

There is no need to collect any additional information.

Synertec will keep this information for 90 days for reporting and tracking purposes and then information will be purged.

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

Geographical area is Kent & Medway

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 our relationship is a Healthcare and patient relationship and they will have limited control. Patients can choose not to have their letters emailed (and will be posted instead). There is no way of "opting out" of Synertec posting their letter. Our patients are expecting us to use their data in this way. We will include children or other vulnerable groups. There are no prior concerns over this type of processing. No it is not novel at any way. Several Kent and Medway organisations are already using this technology and from the same supplier. No public concerns reported. Not applicable as all data will be stored in the UK.

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?
We send appointment letters, consultations outcomes, and discharge letters every day. This is something we are contractually required to do within our contracts; advise patients of discharge, outcome or onward referrals. The aim of this project is to achieve better timeliness of communication to patients, fewer IG incidents arisen from human error and reduction in cost. By outsourcing the mailing process, MCH will see cash releasing benefits of about £30,000 per annum and release 8000 working hours per annum. There also reports that a hybrid mailing solution can reduce DNAs.

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] Data protection officer: [redacted] Caldicott Guardian: [redacted] IT Controller: [redacted] Senior User: [redacted] Expert: [redacted] We haven't consulted with any patient representative. Assurance of impact to patients has been obtained from discussions with other health providers across Kent & Medway who are already using the system successfully.

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?
[redacted] Medway Community Healthcare is the data controller and Synertec is the data processor. Copy of Synertec privacy policy is available. There will be a data sharing agreement in place between Controller and Processor. Without this information it would not be possible to send any correspondence to patients and as a result MCH will not be able treat patients 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. The lawful basis for processing 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. It is not envisaged that the information would be used for other purposes. Supplier contracts and the data sharing agreement prohibit the use of the information for other purposes. Internal rules prevent the use of the information for other purposes.

Step 6: Identify and assess risks

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.

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

No.	Summary of risk	Risk to data subject(s)	Risk to Organisation	Identified risk score	Proposed controls	Residual (target) risk score
1	Synertec may use information outside of the specific published purpose	Privacy risk, damage/distress to individual	Risk to reputation, financial risk (fines) for breaching DPA legislation	M6	Data sharing agreement in place. Advice must be sought from data controller IG leads before using information for any purpose other than that specified	L3
2	Data subjects will not be aware that we are using their information in this way	Privacy risk	Financial risk for breaching DPA legislation	L4	Privacy notice updated. Data sharing agreement will reflect that processors have the same responsibilities as us as controllers. We are not using patient's information in a way we haven't used it before.	L2
3	Letters sent by Synertec via email could be intercepted	Privacy risk	Risk to reputation, financial risk	M8	[redacted]	M4

4	Information may be retained for longer than is necessary by Synertec	Privacy risk, GDPR rights risk	Risk to reputation, compliance risk, financial risk	M6	**Data Storage** Synertec's ISMS policy describes the protection applied to data up to and including the point of despatch, as well as the data storage security measures employed. **Customer-side** Synertec's Prism software is installed on Medway Community Healthcare's server on their network. Document data is accepted by the Prism software and it is assumed that the Medway Community Healthcare will secure this server in such a way as to only allow authorised access. All configuration, processing, routing and storage of document data, occurs on MCH's server. All documents accepted and processed by the Prism software are maintained in an archive 'customer-side' to allow for the review and retrieval of those documents at a later date if required. [redacted]	

					[redacted] Data retention periods are defined according to MCH's requirements and can be varied, if required, by document type. [redacted] **Synertec-side** Segregation of Medway Community Healthcare's data is fundamental to all of Synertec's services for you. Synertec's bespoke systems segregate all data by owner (i.e. customer A's data will be kept separate from customer B's data) throughout the process of moving data into Production. Synertec archives MCH document data for a period of 90 days as standard on its servers. [redacted]	

					[redacted] This archiving allows full traceability of documents for a reasonable period following despatch. Medway Community Healthcare can request that Synertec varies the retention period for a specific reason, if appropriate. [redacted] Synertec do not operate an outsourced data centre. Medway Community Healthcare's data is never stored outside of the U.K, and all Synertec offices, as well as our printing and mailing facilities, are located inside the U.K. **Portable devices** No employee is permitted to store 3rd party (Medway Community Healthcare) data	

					on a portable device or removable media except as a temporary measure when transferring such data between systems within a physical Synertec or Medway Community Healthcare site, or between a Synertec and Medway Community Healthcare site, and only then in pursuance of their duties. Our ISMS Policy mandates that these devices/media must be personally accompanied at all times and must never be transported via a postal or courier service or placed into the hands of any third party.	
5	Error in Synertec IT systems may pull through an incorrect email address which leads to a letter sent to incorrect email recipient	Privacy risk	Risk to reputation, complaint, compliance risk, financial risk	M9	As part of Synertec's commitment to continually provide the most secure environment possible for your data, we strongly recommend that all emailed communication, containing patient identifiable information, is protected with a password. We recommend this regardless of whether it is sent via NHS.net or not, due to the potential for an email to be sent to an unintended/unauthorised	

					recipient. NHS.net addresses cover NHS organisations nationwide as well as commercial third parties. Miss-typing an email address, either when drafting an email or as part of a system configuration, could result in patient identifiable information reaching an unauthorised/unintended recipient and therefore may constitute a serious breach of security. Preventing the incorrect disclosure of patient information and protecting your data's confidentiality is imperative to Synertec. We are constantly reviewing the security measures we have in place with a view to ensuring that your data is as secure as possible. Prism - Password Protected Documents Synertec is able to produce from PRISM password protected documents via email. [redacted]	

					[redacted]	

					Synertec Synertec operates an extensive ISMS system covering its operations for Medway Community Healthcare and it's handling of your data. We enforce that all patient identifiable information that is sent via email from Synertec back to you is encrypted in an attachment in the email. Synertec would then contact you and ensuring that it is correct contact would then provide the password required to open the attachment. The password would never be sent in any email. In the unlikely event that an email was sent to an unintended/unauthorised recipient, the recipient would be unable to open the attachment and the security of patient identifiable information would not be breached.	
6	Synertec IT systems could be infilitrated / hacked	Privacy risk	Risk to reputation, compliance risk, financial risk	M8	[redacted]	

					[redacted]	

					[redacted]	

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.	Action required to implement proposed controls (from step 6)	Approved by IG team	Action owner and target date	Review date	Complete date
2	Check that MCH's privacy notice reflects the use of personal information detailed within this DPIA	Yes	IG manager Aug19	September19	August 2019

Step 8: Sign off and record outcomes

Signed by project lead (person completing the DPIA)

Name: [redacted]

Position: Project Manager

Signed: [redacted]

Date: 15/8/2019

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:

Password protect documents sent from Synertec to patients

Send 2 separate emails: 1x email with the attached password protected letter, and 1x separate email after with the instructions on how to open the letter.

Final sign off

Name: [redacted]

Position: Data Protection Officer

Signed: [redacted]

Date: 15/8/2019