DPIA

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.

Submitting controller details

Name of controller	DOWNLANDS MEDICAL CENTRE 77 HIGh STREET POLEGATE EAST SUSSEX BN26 6AE
Subject/title of DPO	SDHC Pharmacist Consultation Recordings using FourteenFish
Name of DPO (delete as appropriate)	Trudy Slade, NHS Sussex CCG DPO

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:
    - describe the nature, scope, context and purposes of the processing;
    - assess necessity, proportionality and compliance measures;
    - identify and assess risks to individuals; and
    - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

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 aim of the project is to assist Pharmacy staff – who are employed by SDHC but working with SDHC member GP practices under service agreements - in undertaking the required observation of practice in order to pass through their Centre for Pharmacy Postgraduate Education (CPPE) programme assessments. Consultation skills need to be assessed by a GP supervisor. This would usually be done face to face but due to COVID-19 this is not possible. However CPPE are keen that this does not hinder assessments and therefore the option of recording consultations will enable the assessments to proceed. This project will involve recording (audio only) telephone calls between Pharmacy staff and patients with patient consent. The calls will then be listened to by GP supervisors who will assess and provide feedback to the Pharmacy staff. A DPIA is required as recordings will be held which contain personal and special category data regarding patients.

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 processing involves the recording of consultations between Pharmacy staff and a patient. The recordings will take the form of a remote consultation being an audio recording of a telephone consultation. Recordings will primarily be made through the FourteenFish platform, with the option for Pharmacy staff to record using their own device and to then upload the recording to the FourteenFish platform.

The recorded consultation audio streams are transmitted over TLS 1.2 which prevents them from being intercepted. If the patient has consented to recording, then the video and audio data is recording to disk as the consultation is happening. Because the consent process happens before recording begins, if the patient does not consent to recording then nothing is recorded. Recordings are stored on the FourteenFish servers in London (hosted by Amazon Web Services) using AES-256 encryption which is once of the strongest mechanisms available. At no time does any data leave the EU / UK.

Prior to the start of the consultation the Pharmacy staff will be required to complete a two-factor authentication process to access the consultation area of the site. This process will require the Pharmacy staff to enter a telephone number, and to then enter a 6 digit code that is sent via SMS.

The consultation cannot begin until the patient has viewed a consent page, which will clearly explain the purpose and nature of the recording, and the need for the patient's consent.

The consultation is initiated by the Pharmacy staff. They enter a patient's telephone number into the system and this will generate an SMS invite to the patient, informing them that they can now begin their consultation by clicking a link in the SMS message. At the end of the consultation the patient will receive a further prompt with the option to remove their consent if they no longer feel comfortable giving it.

The source of the data is the content of the consultation between Pharmacy staff and patients, who represent the data subjects, and may include detailed discussions of current and historical medical conditions, references to patient notes and previous consultations and other confidential information that may be disclosed in the course of a remote consultation.

This data is therefore of a highly sensitive and personal nature, with a potentially severe impact on the data subject's rights and freedoms in the event of a breach.

To access any recorded consultations, the Pharmacy staff will be required to complete the two-factor authentication process which gives them access to their consultations for 30 minutes.

The recorded content will retained on the Pharmacy staff's FourteenFish user account until they submit selected recordings for review by their clinical GP supervisor. At the point of submission the recorded content will become inaccessible to the Pharmacy staff. At no point are the recorded files available for download – they can only be accessed through the platform following a log in using two-factor authentication.

GP Supervisors will then be granted access to the consultations for the purposes of reviewing and assessing the Pharmacy staff's performance. The consultations can only be reviewed through the platform, and users must again be logged in using two-factor authentication. There is no facility for GP Supervisors to download the recorded consultations.

Each consultation may be accessed by a maximum of two GP Supervisors, and the access rights to the content will be limited so that only specifically allocated GP Supervisors can access the files, and the files will only be accessible during specifically determined time periods. When a GP Supervisor attempts to access a recorded consultation, the system will check several criteria before allowing access; they must be registered as an assessor on the system, they must be logged in using two-factor authentication, and they must have had the specific file in question allocated to them to review. Furthermore, GP Supervisors are required to submit their availability for assessing the consultations, and will only be permitted access during these designated periods of time. Outside of their specific time slot the GP Supervisor will not be able to access any recorded files, even if they have had them allocated.

Once the review and assessment is complete the files will then be permanently deleted from the FourteenFish servers.

The files will be secured with multiple levels of access controls to prevent unauthorised access – this includes preventing access by FourteenFish staff. In the normal course of providing support to users, FourteenFish staff can access user accounts in order to resolve queries, including the facility to "impersonate" a user on the system. The area used for recording and storing recorded consultations is not accessible to FourteenFish staff in this way due to the two-factor authentication process. Files are encrypted at rest using AES-256, meaning a 256 bit encryption key is required to access the files, and this key is controlled by

FourteenFish. The files are also encrypted during transit, using TLS 1.2, which is the strongest commonly available HTTPS protocol.

At no point does the Pharmacy staff have the recording saved on their own device, or a device in the practice. Recordings are always protected using a login (email and password) plus two-factor authentication (SMS to the Pharmacy staff's mobile phone). Recordings always remain on FourteenFish.

If the patient consents to recording, FourteenFish temporarily stores the patient's phone number so that a follow-up message describing how the recording will be used can be sent to them.

Once they have been sent the follow-up message, FourteenFish immediately run their phone number through a one-way encryption process called a cryptographic hash. This is a secure process whereby the phone number gets encrypted in a way that is not reversible, meaning that even FourteenFish or the Pharmacy staff can't get the phone number back even if we wanted to.

However, this hashing process still allows any requests by patients under GDPR legislation to be fulfilled, because if the patient were to tell FourteenFish their phone number then they can run it through the same one-way encryption process and see if we have any consultations that match the encrypted phone number. When the consultation recording is deleted, the hash of the phone number is also deleted.

If the patient does not consent to recording then their phone number, then FourteenFish also immediately delete their number from our system since they don't need to send them a follow-up message, and there would not be a recording made of the call.

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?
FourteenFish will retain this data for the absolute minimum amount of time necessary for the completion of the assessment process before permanently deleting the data. This is estimated to be around three months to allow for the completion of the review and assessment process. Any consultations that are not submitted for assessment will be deleted after 6 months automatically.

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)?
Pharmacy staff will have access to the recorded data up until the point of submission, when the data is made available to at least two examiners to review and mark. At this point the Pharmacy staff can no longer access the data, and it is only available to specific assessors during specific time periods (designated by the data controller). Patients attending the consultations will constitute the data subjects for this processing, and will be asked to give consent at the start of the consultation prior to the commencement of recording. Patients will also be given a clear option to remove their consent at the end of the consultation which will result in the immediate deletion of the data relating to that consultation. Subsequent requests to remove consent will be processed by the data controller. FourteenFish hold ISO 27001 certification, which is audited annually. This certification requires FourteenFish to maintain the highest standards. In terms of data protection and security, and as such we have a robust range of processes and policies designed to minimise or full mitigate the risk of data breaches.

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 goal of the project is to provide a secure, easy to use platform for Pharmacy staff to record and submit their patient consultations for the purposes of CPPE assessment. The requirement for a remote consultation platform has arisen from the limitations on both face-to-face patient contact, and the restrictions on holding face to face assessments, during the Covid-19 pandemic. The benefits of this system for patients will be an easy to access consultation with Pharmacy staff they may not have otherwise been able to visit during the lockdown restrictions. The benefits for Pharmacy staff are that they can practice their consultation skills prior to the submission of their recorded consultations, allowing them to improve their practice and pass

their assessments. At no point does the Pharmacy staff have the recording saved on their own device, and recordings are always protected using a login (email and password) plus two-factor authentication (SMS to the Pharmacy staff's mobile phone). The broader benefits would include the facility to provide a remote consultation platform for Pharmacy staff to use in their daily practice.

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?

A PCN Clinical Director has been approached in principle to discuss the use of this recording facility which was received positively. CPPE has confirmed they are happy for this platform to be used. The Clinical Governance Lead at SDHC has approved its use. Positive feedback has been received from GP Clinical Supervisors regarding the ease of use of the system and its effectiveness to achieve the objective.

Further practices are being approached to ensure they are satisfied that using this system meets all information governance and data requirements.

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 lawful basis for processing personal data is consent (a) consent. The lawful basis for processing special category data is (a) explicit consent. Patients are given information to ensure they are aware of their rights, how the data is held and used and that they know they can withdraw their consent at any time, the right to be forgotten, the right to have a copy of the recording. We are satisfied that the Fourteen Fish system is suitably encrypted and used with data security and protection issues in mind.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1. Pharmacy staff could share their login details	Possible	Significant	Medium
2. Recordings could be overheard by others depending on the environment in which the Pharmacy staff are working	Possible	Significant	Low
3. Patients may change their mind and withdraw consent to use the consultation, after it is recorded	Possible	Significant	Medium
4. Fourteen Fish platform could be hacked.	Remote	Severe	Low

10

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**	**Residual risk**	**Measure approved**
		Eliminated Reduced Accepted	**Low Medium High**	**Yes/no**
1.	This would be in contradiction to the SDHC policies surrounding data security and would be a disciplinary offence	Reduced	Low	Yes
2.	Staff usually use earphones and are aware of data security issues	Reduced	Low	Yes
3.	Ensure patients are informed that they can contact their practices if they wish to withdraw their consent at any time	Reduced	Low	Yes
4.	SDHC and the GP practices involved will need to rely on Fourteen Fish's data security procedures which appear to be robust.	Accepted	Low	Yes

Step 7: Sign off and record outcomes

<table>
<tr><th>Item</th><th>Name/position/date</th><th>Notes</th></tr>
<tr><td>Measures approved by:</td><td>Kirstie Ingram, SDHC Chief Pharmacist and Andrea Fear, SDHC DPO</td><td>Integrate actions back into project plan, with date and responsibility for completion</td></tr>
<tr><td>Residual risks approved by:</td><td></td><td>If accepting any residual high risk, consult the ICO before going ahead</td></tr>
<tr><td>DPO advice provided:</td><td>Trudy Slade</td><td>DPO should advise on compliance, step 6 measures and whether processing can proceed</td></tr>
<tr><td colspan="3">Summary of DPO advice: The practice should understand that they will lose control over any data that is uploaded to the Fourteen Fish site, and that patients should be made aware where to contact to exercise their individual rights, such as right to restrict processing, and subject access request.

The practice should ensure that they note the data flow on their data flow map and update their privacy notice to reflect the activity.

<table><tr><td>Pharmacist Training</td><td>Purpose – Personal confidential and special category data will be collected and used to inform and assist with the assessment of pharmacists working in the surgery. No data will be shared unless the patient has consented.

Legal Basis : under GDPR Article 6 1 (a) consent

Article 9 2 (a) explicit consent

Processor: Fourteen Fish</td></tr></table></td></tr>
<tr><td>DPO advice accepted or overruled by:</td><td></td><td>If overruled, you must explain your reasons</td></tr>
<tr><td colspan="3">Comments:</td></tr>
</table>

Consultation responses reviewed by:	Trudy Slade, NHS Sussex CCG DPO	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Practice Manager in consultation with Kirstie Ingram, SDHC Chief Pharmacist	The DPO should also review ongoing compliance with DPIA