Royal College of General Practitioners

Data Protection Impact Assessment Procedure

Contents

1 Version Control

Version	Description	Date	Author	Reviewer
1.0	Approved for Issue	21/01/19	Data Protection Officer (DPO)	DPO

2 Procedure Owner

The Owner of this procedure is the DPO.

3 Purpose

To comply with the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; the GDPR, the Law Enforcement Directive (Directive (EU) 2016/680); any applicable national implementing Law as amended from time to time; and all applicable Law about the processing of personal data and privacy; when the RCGP enters into any data processing operation.

4 Scope

All projects that involve processing personal data, or any activities that affect the processing of personal and impact the privacy of data subjects are within the scope of this procedure and may be subject to a data protection impact assessment (DPIA).

5 Responsibilities

The DPO is responsible for performing the necessary checks on personal data to establish the need for conducting a DPIA.

The Senior Responsible Owner (SRO) is responsible for ensuring appropriate controls are implemented to mitigate risks identified as part of the DPIA process.

6 Procedure

The Data Protection Officer / Project Manager / Programme Office identifies the need for a DPIA at the start of each project. The type of personal data involved, and processing activity, are screened against the questions set out in this procedure.

a. Screening checklist.

We consider carrying out a DPIA in any major project involving the use of personal data.

Carry out a DPIA if you plan to implement any of the following types of processing:

Evaluation or scoring;

automated decision-making with significant effects;

systematic monitoring;

processing of sensitive data or data of a highly personal nature;

processing on a large scale;

processing of data concerning vulnerable data subjects;

innovative technological or organisational solutions;

processing that involves preventing data subjects from exercising a right or using a service or contract.

Always carry out a DPIA if you plan to:

Use systematic and extensive profiling or automated decision-making to make significant decisions about people;

process special-category data or criminal-offence data on a large scale;

systematically monitor a publicly accessible place on a large scale;

use innovative technology in combination with any of the criteria in the European guidelines;

use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

carry out profiling on a large scale;

process biometric or genetic data in combination with any of the criteria in the European guidelines;

combine, compare or match data from multiple sources;

process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

process personal data that could result in a risk of physical harm in the event of a security breach.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

b. The template in Appendix 1 will be used to record all DPIAs.

Appendix 1

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.
Currently the COVID-19 pandemic has made it impossible for trainees to complete training via the normal route, blocking the pipeline of GP's into the workforce and creating future patient safety issues due to a potentially diminished workforce. The Recorded Consultation Assessment (RCA) Core Group was formed on 1st May in response to call from both HEE and the RCGP to help resolve this issue. It is proposed that a 'Recorded Consultation Assessment' (RCA) should replace CSA for the summer 2020 diet and, if necessary, for any future diet if Covid19 restrictions continue/re-cur. The RCA is proposed as a pragmatic compromise with safeguards in place to ensure, both that the standards for assessing readiness for independent practice as a GP in the NHS are not lowered, and with a view to ensuring that pass/fail rates are in line with norms for the CSA. The RCA is a summative assessment of a doctor's ability to integrate and apply clinical, professional, communication and practical skills appropriate for general practice. It uses pre-recorded video or audio consultations to provides evidence from a range of encounters in general practice relevant to most parts of the curriculum and also provides an opportunity to target particular aspects of clinical care and expertise.

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 a GP Trainee and a patient. The recordings may take the form of a remote video consultation, a recording of a face-to-face consultation, or an audio recording of a telephone consultation. Recordings will primarily be made through the FourteenFish platform, with the option for trainees to record using their own device and to then upload the video to the FourteenFish platform. In order to register the trainee will be required to submit a photograph in order to verify their identity, which is confirmed by their allocated supervisor. This process is to ensure the account owner is the same user who is recording the consultations. Facial recognition software can then be used to verify the users in the recorded videos, and will flag up any anomalies to the supervisor. The recorded consultation streams (comprising the patient's video and the GP trainee's video) will be initially hosted by a third party (Twilio, based in Ireland). Once the consultation is ended we instruct Twilio to combine the 2 streams into a single video file. This process takes around 5-10 minutes. Once complete we are then notified by Twilio, and we then securely transfer this file on the FourteenFish servers (hosted by Amazon Web Services in London). The files are transferred directly from Twilio's servers, using a secure upload link that we control. Twilio will then permanently delete the files from their servers, including metadata. Prior to the start of the consultation the trainee will be required to complete a 2-factor authentication process to access the consultation area of the site. This process will require the trainee 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. It will also be made clear that this consent can be withdrawn by the patient at any time, and the process for this will make it as easy to remove consent as it is to give it. The consultation is initiated by the GP Trainee once they have logged in and completed 2-factor authentication. They can then 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 GP trainee 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, physical examinations, and other confidential information that may be disclosed in the

course of a medical 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.

The recorded content will retained on the trainee's user account until they submit selected recordings for review by the RCGP examination team. At the point of submission the recorded content will become inaccessible to the trainee. At no point are the recorded files available for download - they can only be viewed through the platform following a log in using 2-factor authentication.

RCGP Examiners will then be granted access to review the consultations for the purposes of grading the trainee's performance. The consultations can only be reviewed through the platform, and users must be logged in using 2-factor authentication. There is no facility for Examiners to download the recorded consultations.

Each consultation may be reviewed by two examiners, and the access rights to the content will be limited so that only specifically allocated examiners can access the files, and the files will only be accessible during specifically determined time periods agreed with the College. When an examiner attempts to access a recorded consultation, the system will check several criteria before allowing access; they must be registered as an examiner on the system, they must be logged in user 2-factor authentication, and they must have had the specific file in question allocated to them to review. Furthermore, examiners 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 examiner will not be able to access any recorded files, even if they have had them allocated.

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

The files will be secured with multiple levels of encryption to prevent unauthorised access – this includes restricting access to administrator users within FourteenFish. 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 and would still require 2-factor authentication to access. 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.

For uploaded consultations, the RCGP is not the data controller until the trainee uploads the consultation to the Remote Consultation tool. Prior to this point, as recordings may never be used for the exam, or might have originally been recorded for a different purpose, the trainee will need to comply with their existing practice data protection and control processes, and during this period the data controller will be the same as for similar non-RCA recordings made within the trainee's practice.

Once a consultation has been uploaded to the Fourteen Fish recorded consultation system, as with recording made through the Fourteen Fish platform, the RCGP will become the data controller of the consultation within the system, and it is strongly recommended that all other copies of the consultation are deleted.

The patient will need to be able to contact the RCGP for access and deletion if they do subsequently decide to remove consent. As a result, when uploading we clearly need the trainee to offer assurance that consent has been obtained and that it exists on the recording verbally, or via other appropriate evidence, and patients will need to be made aware of who to approach to fulfil their rights.

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 two months to allow for the completion of the examination and review process.

Any consultations that are not submitted for assessment in the RCA will automatically be deleted after three months.

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)?

GP trainees 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 trainee can no longer access the data, and it is only available to specific examiners 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 trainees to record and submit their patient consultations for the purposes of the RCA Examination. The requirement for a remote consultation platform has arisen from the limitations on both face-to-face patient contact, and the restrictions on holding on-site examination days, during the Covid-19 pandemic.

The benefits of this system for patients will be an easy to access consultation with a doctor they may not have otherwise been able to visit during the lockdown restrictions. The benefits for trainees are that they can practice their clinical and consultation skills prior to the submission of their recorded consultations, allowing them to improve their practice and pass their professional exams. The broader benefits would include the facility to provide a remote consultation platform for qualified GPs and other healthcare professionals 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?
The RCA Core Group was formed on 1st May in response to call from both HEE and the RCGP. There has been constant comms & consultation to all relevant stakeholders since this date with regular updates on both the RCGP and FourteenFish websites.

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 bases for processing are Public Task and Legitimate Interests. Processing is necessary to ensure continuing GP Trainee assessment during the coronovirus pandemic. The processes, and application, have been developed in conjunction with NHS Digital. The data processor, FourteenFish, is subject to a data processing agreement between them and the RCGP. Information will be provided to patients prior to the recorded consultation taking place. Information will be sufficient to enable the patient to either provide consent, or not provide consent. Without consent the assessment will not proceed. Data subject rights will be managed by the RCGP and the trainee's GP Practise. At all times both the RCGP, and the GP Practise, will ensure patients are informed of how the processing works and their rights in relation to the processing.

Step 5: Identify and assess risks

Likelihood of harm/severity of harm	Minor risk (1)	Reasonable risk (2)	Significant risk (3)
Low (1)	Low	Low	Low
Medium (2)	Low	Medium	High
High (3)	Low	High	High

Risk	Likelihood of harm	Severity of Harm	Overall risk
Access to personal data from unauthorised user	Low	Significant	3-Low
A GP Trainee makes a recording outside of the system for uploading using their own device and the device/platform used is compromised or stolen	Low	Significant	3-Low
A GP trainee or Supervisor stays logged in on a shared device allowing another unauthorised user to access the data	Low	Significant	3-Low
Integrity of devices used to access the platform (how at risk are they from Trojans/Viruses	Low	Minor	1-Low
Third party data visible on desks/screens during video consultation that may be viewed/captured during the recording	Low	Minor	1-Low
A third party is present in the room of one of the video consultation participants without the other participant knowing	Low	Significant	3-Low
A third party clandestinely accessing the call via by guessing the URL	Low	Significant	3-Low

Step 6: Identify measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Access to personal data from unauthorised user	In order to access the area of the site where recordings are made and stored, the trainee must log in using 2-factor authentication. In order for an examiner to access recorded files they must be registered as an examiner, log in using 2-factor authentication, have the file allocated to them, and can only access it during a previously designated time period. System and app logs will be retained for investigative purposes in the unlikely event of a breach. These will be retained for 12 months and will not be proactively analysed.	Reduced	Low	Yes
A GP Trainee makes a recording outside of the system for uploading using their own device/software	Trainee can complete the recording using their own device and software, and during this period will be considered the data controller. The trainee will be bound by their standard probity requirements to ensure patient confidentiality, including the deletion of videos after uploading to the platform	Unmitigated risk	Unmitigated risk	n/a
A GP trainee or Supervisor stays logged in on a shared device allowing another unauthorised user to access the data	Session times out after 60 minutes using a sliding expiration cookie. Following the expiration of this cookie the user will be required to complete the 2-factor authentication process again in order to continue using the site.	Reduced	Low	Yes
Integrity of devices used to access the platform (how at risk are they from Trojans/Viruses	Use of devices (laptop & desktop computers) that comply with NHS standards of encryption	Reduced	Low	Yes
Third party data visible on desks/screens during video consultation that may be viewed/captured during the recording	The GP trainee recording the consultation and their supervisor can review the recorded material and delete the file if it contains third party information	Reduced	Low	Yes

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A third party is present in the room of one of the video consultation participants without the other participant knowing	Patient can ask the GP trainee to scan the camera around the room to alleviate concerns about third parties being present	Reduced	Low	Yes
A third party clandestinely accessing the call via by guessing the URL	The system provides an end to end system that cannot be joined by a third party, in the unlikely event they were able to guess the unique URL of the call, and join at the exact same time as the participants are on the call	Eliminated	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Jon Harrex, Data Protection Officer, June 22 2020.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Jon Harrex, Data Protection Officer, June 22 2020.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: See options in stage 6.		
DPO advice accepted or overruled by:	Chris Mirner, Assistant Director for Postgraduate Training, June 22 2020	If overruled, you must explain your reasons

Comments: Accepted		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Chris Mirner, Assistant Director for Postgraduate Training, June 22 2020	The DPO should also review ongoing compliance with DPIA