DPIA review intellin

This template 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.

Submitting controller details

Name of controller	Rory Cameron
Subject/title of DPO	Mr
Name of DPO	Rory Cameron

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.
We want to help people with diabetes better manager and understand their diabetes whilst also preventing or slowing down their progression to having complications from their diabetes. Intellin is an app based platform where an individual can input or pull in personal medical information in order to better manage their diabetes. These data can also be shared with their clinical team. The data sets are also used to create algorithms to predict the risk of developing complications and to publish clinical findings that improve the understanding of diabetes. DPIA is necessary as we are processing '**biometric data', 'sensitive data', 'data concerning vulnerable data subjects' and 'data is processed on a large-scale'.**

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?
Data is collected and inputted by the patient or automatically through api connections to other health platforms. The data can be shared with their healthcare professional. Patients will be able to see their risk of developing complications from their diabetes. The data will be reviewed for publication in medical journals. Data is stored with Amazon Web Services. Data is backed up to a hard drive. If asked by the patient. We can delete their email from the database and replace this with the word 'deleted' followed by the key of the database row. Thus deleting them from the dataset. There is no tracking on the app. Permission is asked for to send push notifications.

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 we collect is around clinical markers linked to diabetes and cardio metabolic disease in addition to ethnicity, age, sex and top level geographical data (not geo location, but region of residence). We collect data every 15mins as and when new data is inputted and it is stored for as long as is necessary to fulfill the purposes for which it is collected. By law we have to keep basic information for 6 years for tax purposes. We have over 9 thousand active users and we expect this to scale to into the 100s of thousands globally.

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)?
We collect data on adults with diabetes. They have full control of what they input and they also have to give active permission and link any devices or apps to our platform. All the data we collect is explicit and clearly listed. The data we collect are already collected by many other devices and apps and we are certified ISO 27001. There a no ongoing issues of public concern about sharing an individuals data with them to help them manage their diabetes. Data is only shared with their healthcare professional if they consent and generate a code for their healthcare team. Publication of data will only be done to look at trends in the anonymised data sets and to understand how metabolic markers change over time.

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 want to help people manage and track their diabetes management. We want to enable people to be remote reviewed or managed by their healthcare team if they active this. We want to educate people on how their metabolic markers can predict how they may develop complications from their diabetes. We want to use this generations anonymised data to improve the outcomes for future generations with diabetes. We want to develop new algorithms to predict the risk of developing complications to enable to resource planning and allocation by those delivering healthcare such as the NHS. We want to help people capture their data by automating this with connections to other devices and apps with their active consent.

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?
We have discussed these at length with our Clinical Advisory Board, Our patient panel and market research we completed in Greater Manchester, In addition these were all reviewed as part of our ISO27001 accreditation. As we grow as an organization we will be recruiting a Regulatory head to further embed these policies and processes into the organization.

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?
We process data on behalf of the person with diabetes to help them better manage their condition. This is only done at their request by them actively downloading and installing our platform. There is no other way to capture the data for people so that they can manage their diabetes. Any new functionality within the intellin platform that may result in changes to our data processing will only occur with direct input from patients and healthcare professionals and a DPIA review will be conducted in advance. All information we collect is inputted by the individual. Data coming from third party apps and devices is assumed to be correct. Before we update or perform any change the to the app or code we ensure that we ask the question 'do we need to complete a DPIA assessment'. No work will start unless this discussions has taken place.

Our data is only stored in the UK with AWS along with the backup.

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**
Data coming from a third party app or device may not be accurate. We only connect to registered medical devices or reputable app brands such as; OMRON, Fitbit etc see complete list here https://support.intellin.com/docs/list-of-compatible-apps-and-devices	Remote	Minimal	Low
Our AWS data base has a data breach. Low likelihood with all their security measures.	Remote	Severe	Low
Backups are stolen. These are kept in a secure location within a fireproof locked safe.	Possible	Significant	Low
Someone access the intellin app on the phone. We cannot control if people have a password on their phone, so if someone access the phone they could access the information in intellin	Possible	Minimal	Medium
Rogue member of staff downloads database. Having a small team with clear processes in place mitigates this risk but as we grow as an organization. Currently it is only the lead developer who can access this.	Remote	Severe	Medium

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**
Medium	Someone access the intellin app on the phone. We could in the future ask users if they want finger or face id to access the app on the phone.	Accepted	Low	Yes
Medium	Rogue member of staff downloads database. As the team grows we need to ensure we have a hierarchy of who can access the database in addition to the current password protections.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Chris Genders CPO 06/03/2020	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Chris Genders CPO 06/03/2020	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Rory Cameron CEO 06/03/2020	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The team needs to continue to ensure we only collect data that is required and asked for by the patient and also to ensure we maintain the high standards on connected to CE marked devices or reputable apps. I will ensure DPAI remains for of mind for the company.		
DPO advice accepted by:	Chris Genders CPO 06/03/2020	If overruled, you must explain your reasons
Comments: Advice given is 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:	Rory Cameron CEO	The DPO should also review ongoing compliance with DPIA