

Regulatory Sandbox Final Report: Novartis Pharmaceuticals UK Ltd

A summary of Novartis' participation in the ICO's Regulatory Sandbox Beta

Date: 5th February 2021

ico.

Information Commissioner's Office

Contents

1. Introduction.....	3
2. Executive summary	4
3. Product description	7
4. Key data protection considerations.....	8
5. Ending statement.....	16

1. Introduction

- 1.1 The ICO introduced the Sandbox service to support organisations who are developing products and/or services that use personal data in innovative and safe ways and where such products and/or services deliver a potential public benefit.
- 1.2 In order to develop the Sandbox, the ICO initially launched the Sandbox as a beta phase, for an initial group of participant organisations during 2019 – 2020.
- 1.3 The beta phase provided a free, professional, fully functioning service for ten organisations, of varying types and sizes, across a number of sectors.
- 1.4 Organisations who were selected for participation in the Sandbox beta phase have had the opportunity to engage with the ICO; draw upon expertise and receive advice on mitigating risks and implementing 'data protection by design' into their product or service, whilst ensuring that appropriate protections and safeguards are in place. Novartis Pharmaceuticals UK Limited ("Novartis") was one of the candidates selected for participation in the Sandbox beta phase.
- 1.5 Novartis is a leading medicines company, using innovative science and digital technologies to create transformative treatments in areas of great medical need.
- 1.6 The ultimate goal of the Novartis project is to make great patient care easier and more efficient, such as by enabling clinicians to access data about their patients' conditions remotely, as well as being able to share information with their patients. Within the Sandbox, Novartis developed a 'Digital Solution' use case that allows patients to provide Patient Reported Outcome Measures ('PROMs') to their clinician by completing pre-set, bespoke, validated health questionnaires from home. These PROMs will provide clinicians with additional insight into their patients' symptoms remotely, and enable greater and more effective clinical-decision making.
- 1.7 This development forms part of a larger piece of Novartis' exploration of the use of voice technology. Novartis' original vision, on entry to the Sandbox, was to voice-enable the software, allowing users (clinicians and patients) to interact with a

digital assistant as an interface, by speaking into the user portal, to set reminders for patients, or to answer health questions. This vision was based on research performed with a range of healthcare professionals, who felt that voice technology, when used effectively, could reduce time spent typing, looking up data, or switching between different NHS systems manually. The use of such technologies is rapidly expanding in the consumer sector, with many households utilising well-known voice enabled 'smart' devices within homes, or enabled on mobile devices. While there are many examples of consumer use cases for voice enabled technology, the use of such technology in the healthcare sector is in its infancy in the UK.

- 1.8 In order to address any perceived data protection concerns associated with the deployment of voice enabled technologies, particularly in a sensitive, clinical setting, Novartis applied to enter the ICO's Regulatory Sandbox. Novartis was accepted into the Sandbox on 1 July 2019 and a Senior Case Officer was appointed. The Senior Case Officer attended Novartis' offices on 30 July 2019 to gain an insight into the organisation and the proposed solution, and to begin formulating the objectives and tasks of Novartis' bespoke Sandbox plan. The content of Novartis' Sandbox plan was agreed by Novartis' Head of UK Data Privacy (UK & Ireland) and approved by the ICO's Sandbox Commissioning and Advisory Group on 16 October 2019.
- 1.9 During its time in the Sandbox, Novartis has received steers from the ICO including, in relation to the controller-processor relationships within the defined supply chain, and the risks associated with the deployment of automated technology within clinical settings. Steers were also provided on the privacy implications of using a digital voice enabled solution in clinical settings, particularly rheumatology and dermatology clinics. This report outlines the work that the ICO Sandbox team supported Novartis with during its time in the Sandbox Beta.

2. Executive summary

2.1 Novartis' Sandbox plan agreed objectives were as follows:

- **Objective 1:** Novartis, with assistance from the ICO Sandbox, would map the data flows relating to use of the Digital Solution in different clinical scenarios, to establish the data protection implications of each scenario, in order to identify

appropriate use-cases for testing within the Sandbox and for deployment in real-world clinical settings.

- **Objective 2:** Novartis, with assistance from the ICO Sandbox, would establish whether any of the processing associated with the explored use-cases identified in Objective 1 above, are subject to Article 22 of GDPR: Automated decision-making and profiling. This would include consideration of the restrictions imposed by Article 22(4). Novartis would ensure that appropriate controls and safeguards are implemented to protect the rights of individuals.
- **Objective 3:** Novartis and the ICO Sandbox would establish whether any speech/voice data collected by the Digital Solution could be defined as 'biometric data' or 'special category biometric data' and would ensure appropriate controls and safeguards were implemented as necessary.
- **Objective 4:** Novartis, with assistance from the ICO Sandbox, would explore the data protection roles (eg 'data controller', 'joint data controller', 'data processor') and responsibilities of itself and of other parties involved in the processing of personal data once the end Digital Solution is rolled out into real-world clinical settings. Dependent on the outcome of this work, Article 6 lawful bases and Article 9 GDPR / Schedule 1 of the Data Protection Act 2018 conditions for processing in the context of special category data would also be explored.
- **Objective 5:** Novartis, with assistance from the ICO Sandbox, would identify technical and organisational measures to protect the security and integrity of the personal data being processed by the Digital Solution. This would likely include, carrying out due diligence checks of third party technology providers, and considering encryption and access controls, and end-user training and awareness.
- **Objective 6:** Novartis and the ICO Sandbox would seek to identify and understand both the beneficial and challenging implications of utilising voice technology in real-world clinical settings.

2.2 Through regular meetings, attendance at project sprints and workshops, the ICO Sandbox provided support to Novartis to address some of the data protection challenges posed by the development of the Digital Solution for use in the NHS,

including discussion of the risks posed by using voice technology as an interface for processing of health data in clinical settings.

- 2.3 Through its Sandbox participation, it was established that Novartis would not have an official data protection role in regards to the personal data processed via the Digital Solution following its deployment in the NHS (as discussed in 4). Although Novartis is not considered as a controller or processor in this context, it was believed to be imperative for the Digital Solution to be designed with data protection in mind to provide the NHS with necessary assurance of the Digital Solution's compliance and protection of data subjects' health data. A preliminary data protection impact assessment and a privacy notice were also drafted with support through the Sandbox, to provide the NHS with a 'ready-made' Digital Solution, and to partly reduce the burden on the NHS to consider all of the risks posed, and the time spent to develop some of the appropriate documentation.
- 2.4 Due to a change in Novartis' and its NHS clients' business priorities in response to the COVID-19 pandemic, Novartis took the decision to offer its Digital Solution to the NHS without the voice aspect of the technology enabled. This is because, the pandemic had highlighted the importance of providing clinicians with a solution that allows remote monitoring of patients (via the sharing of PROMs), in order to reduce in-person footfall in clinics. Although the implications of processing voice data have been explored in the Sandbox, the necessary work to technically voice-enable the Digital Solution has not been carried out in sufficient time to allow its deployment in Q1 of 2021. At launch, users interact with the Digital Solution by typing commands and responses into the portal rather than interacting with it through speech.
- 2.5 As it was established during its Sandbox participation that Novartis would not be a controller or processor following the deployment of the Digital Solution into NHS bodies, and that the Digital Solution would not be voice-enabled as initially planned, some aspects to the Objectives above were not able to be fully completed. For example, considerations around lawful bases were not considered in detail because they apply only to data controllers, and Novartis was deemed to not be a controller or processor. All aspects of the Objectives were discussed conceptually to support Novartis in the design of a voice enabled solution in the future.

- 2.6 Novartis has communicated its intent to the ICO to revisit the learnings gleaned through its Sandbox participation in the future to design a voice-enabled solution for use in clinical settings.

3. Product description

- 3.1 Early in the project, Novartis engaged with a number of healthcare professionals (both doctors and nurses) to understand their day-to-day experience with their patients. This provided valuable insight to understanding what use cases in relation to the Digital Solution may add maximum value to facilitating high-quality clinical decision making and streamlining otherwise time-consuming tasks.
- 3.2 A number of use cases were explored and the data protection risks of each were examined as part of the Sandbox engagement. It was felt that a valuable solution would allow clinicians to share information with their patients, and provide efficient access to data about their patient's symptoms remotely. Novartis therefore developed a use case to allow patients to provide Patient Reported Outcome Measures ('PROMs') to their clinician by completing health questionnaires digitally from home. Clinicians will use existing validated questionnaires depending on the individual patient's condition, as well as reminders to notify the patient to complete the questionnaires. This solution will allow clinicians to efficiently draw upon this data, examine any changes to their patient's condition and allow prioritisation of those individuals who need to be seen more urgently in clinic.
- 3.3 Novartis and healthcare professionals involved in the project also had a vision to voice enable the Digital Solution so that users (both patients and clinicians) could interact with it by speaking rather than typing in commands or responses. One use case identified by healthcare professionals involved remote monitoring of a patient's adherence to their medication. Using the Digital Solution, the clinician would begin by asking their device to retrieve data about a patient, and a voice processing interface would translate their speech into machine readable text. The Digital Solution would then send an alert to the patient and remind them to provide certain information. After providing the information verbally, the patient's speech would be turned into data for the clinician to view within their portal.

- 3.4 Novartis engaged with a number of technology vendors to support the development and design of the Digital Solution. A particular vendor, an established NHS technology provider, was selected to build the web portal component to the solution under Novartis' instruction. The Digital Solution has been designed as a web application, providing both a patient-facing portal and a clinician-facing portal, with data stored on the NHS network. Novartis is currently working with relevant NHS bodies to implement the solution in a number of NHS Trusts and Health boards in early 2021.
- 3.5 During the Sandbox engagement, Novartis also engaged with a number of voice technology vendors in relation to the voice component of the Digital Solution. These vendors included the owners of large voice technology platforms, as well as smaller organisations that build on top of existing voice technology solutions. By partnering with these vendors, Novartis aims to build and deploy a voice enabled solution that is scalable and meets the needs of the clinicians and patients.
- 3.6 In light of the Coronavirus pandemic, Novartis identified that delivering a tool, to provide clinicians with the ability to monitor their patients remotely and to reduce unnecessary face-to-face appointments was more urgent in the immediate term. In this context, a decision was made by Novartis to implement the solution, without a voice element, in order to support the NHS and its patients during the COVID-19 crisis and beyond. Although the Digital Solution is not voice-enabled at this time, Novartis will take the learnings from the Sandbox process to revisit the use of voice technology in the future, as part of its overall data and digital strategy.

4. Key data protection considerations

Roles and responsibilities

- 4.1 It is imperative that an organisation understands its role in relation to the personal data which it processes. This is key to ensuring compliance with data protection law, as well as upholding the rights and freedoms of the individuals that will be affected. Due to the complexity of real-world business relationships, especially in technology supply chains, it is not always clear which party(s) are the 'controller' and which are the 'processor'. Two or more parties may be considered as 'joint

controllers', and others, often the developer of a product or solution (who does not actually process any personal data but simply supplies the product or solution to a customer), may not hold a data protection role at all once the end product is sold to a client or implemented in the real world.

- 4.2 One of the first challenges that Novartis and the ICO worked to resolve in the Sandbox was the matter of controllership. It was agreed that the NHS body where the Digital Solution would be implemented such as a Trust associated with a hospital or a GP practice, would be regarded as a controller. This is because the clinicians using the product employed by the NHS body will have a designated statutory and legal duty to treat and care for patients. It is the relevant NHS body who will have the end relationship with the patients accessing the patient-facing portal.
- 4.3 Discussions in the Sandbox took place in relation to whether Novartis could be considered as a joint controller alongside the relevant NHS body. The reasons for this were due to Novartis making decisions about the design of the solution, whilst engaging with stakeholders including clinicians employed by the NHS. Novartis would also make decisions specifically about what personal data fields patients will be asked to complete within the portal to ensure the utility of the Digital Solution, therefore it will have significant influence over the means of the processing. In addition, Novartis considers itself to have a general common objective with the NHS, another indicator of joint controllership, specifically an interest in improving patient treatment and care.
- 4.4 Although the product design may be considered as a joint venture between Novartis and the relevant NHS body, through significant engagement, the business relationship between two parties may not indicate a joint controller relationship as it is defined by the GDPR. This is because the Digital Solution aims to facilitate and improve upon NHS services and offers a more efficient 'means' through which to carry out patient care and treatment, processing already carried out by the NHS and its employees. The relevant NHS body will be ultimately responsible for deciding whether to implement the solution, and clinicians will be required to exercise their professional judgement in deciding which patients should be allowed access to the portal and in making clinical decisions about the patients' care and treatment as a result. Therefore, the NHS body will be the determinant of both the purposes and the means that patient data is processed by in line with its statutory obligations, in the context of patient care, and can be considered the controller in this context. The NHS body will also be the party responsible

for determining its Article 6 lawful basis for processing and the Article 9 conditions for processing of any special category data, deciding on retention of the data, amongst other controller obligations.

- 4.5 Further to this, Novartis has recruited a technology partner to configure a solution under the instructions of Novartis at the product design stage. This partner will also operate and maintain the Digital Solution under the NHS body's instructions once it is deployed in practice. This partner would therefore be considered a data processor and a data processing contract will exist between the NHS body and the technology partner. Once deployed, Novartis will have no access to patient data acquired and processed through the Digital Solution, and is therefore unlikely to be considered as a processor, and will not have a data protection role. Nonetheless, Novartis need to ensure that the design and manufacture of the solution is carried out in a manner which takes account of the GDPR, and incorporates data protection by design and default.
- 4.6 Regardless of its role in terms of the end Digital Solution, Novartis has ensured that the Digital Solution has been built to take into account the controller's obligations and that risks to data subjects are considered in development stages. The ICO would recommend to other organisations, that where there is an ultimate aim to process personal data, that each organisation involved in the supply chain considers Article 25 of the GDPR, 'data protection by design and default', and Recital 78, in the development of their products and services.

The processing of voice, speech and biometric data

- 4.7 The original design of Novartis' Digital Solution involved a voice interface. Clinicians could set reminders for their patients to complete health assessments, or could pull up data about how a specific patient's condition had changed over previous weeks, by speaking into the clinician-facing portal. Likewise, patient users could complete health assessments by giving their answers verbally into the patient-facing portal.
- 4.8 An individual's voice data may be considered as 'biometric data' under Article 4(14), 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'. Voice data may also be considered as 'special category' where it is

used 'for the purpose of uniquely identifying an individual'. This would require consideration of Article 9 / Schedule 1 of the DPA 2018 and an organisation would need an appropriate condition for processing where this is the case.

- 4.9 Novartis requested a steer from the ICO during its time in the Sandbox, to determine in what circumstances, when somebody speaking into a voice-enabled device, would that individual's voice be considered as 'biometric data' and further when it would be considered as 'special category' and require a condition for processing. Novartis was keen to know this, so that it was able to engage with relevant NHS bodies to provide assurance about the intricacies of the processing and examine any risks to data subjects from early design stages.
- 4.10 Novartis would be procuring a technology vendor to supply the voice processing component to the solution. Whether an individual's speech data is considered as biometric data would depend on what the technology provider was 'doing' with that audio data, and how it was being technically processed. It was agreed that 'speech' and 'voice' could be broken down into two different concepts. Where 'speech' can refer to what somebody is saying, 'voice' can describe how an individual speaks. If a technology vendor is simply extracting the content of somebody's speech to understand what they are saying to enable the solution to work, it isn't necessarily processing any data about an individual's voice. Although the content of the words could be personal data, especially where a patient is providing data verbally about their health condition, the technology would not gather data about an individual's vocal characteristics or the way that they speak. On the other hand, if a technology vendor is technically processing information about the vocal characteristics of an individual to learn something about the way they speak, or to allow a distinction between that speaker and another, this would be 'biometric data'.
- 4.11 Where that biometric data is then used for the purposes of authenticating that individual based on their voice patterns and characteristics, this would be considered special category data. Voice authentication may be used as an additional access control for logging into a system. An example of this in the consumer market, is opting in to 'voice matching' when using a smart device at home, in order to access personalised services, or to distinguish yourself from another user in the same household. Novartis decided that voice authentication would not be a necessary component to design into a Digital Solution after a discussion about the proportionality and necessity of processing special category biometric data in the context of health care.

- 4.12 Providers of well-known voice-enabled 'smart devices' in the consumer market may collect biometric data from users to train their speech recognition models in order to reduce errors. Although this may be classed as biometric data because it is data about the way an individual speaks, it will often be pseudonymised, therefore it is not being used to uniquely identify that speaker and is not special category.
- 4.13 Although it was agreed that the processing of speech data (what the user is saying), would be integral to the solution, Novartis would need to engage with its chosen voice vendor to understand the intricacies of the processing and whether it is collecting users' biometric data for its own purposes and whether there is an option to opt out of this process to restrict the amount of personal data being collected about users. Where a vendor, that would usually be considered as a processor, is collecting and processing data for its own purposes beyond those instructed by the controller, eg for model training purposes, it would become a controller in its own right and would be required to comply with all of the GDPR controller obligations including having an appropriate lawful basis. In the context of healthcare, where sensitive health information is also likely to be collected during the course of speech and voice data collection, due to the nature of the Digital Solution's use, the technology vendor would need to agree specific parameters and additional safeguards with the healthcare body eg the NHS body, for this collection and secondary processing, due to the added risks involved. Any such processing that is not agreed with the relevant body would be unlawful.
- 4.14 An additional steer was provided to Novartis to outline the different risks that could occur when using voice enabled technology. This was intended to support its due diligence of the different voice technology vendors that it may choose to partner with in the future. Some of these additional considerations are as follows.
- How will the solution be activated? Devices that are activated by a user speaking a 'wake word', continuously listen for the acoustic pattern that matches that trigger word. These devices are often referred to as 'always on'. Although assurances have been provided by some well-known voice vendors, that speech or background noise is stored on-device (not sent up to the cloud) and then deleted within seconds, when the device is mistakenly awakened by incorrectly recognising the trigger word, this audio will be sent up to the cloud for additional processing. This process risks breaching both 'fairness and transparency' Article 5(1)(a) and the 'data minimisation' principles, Article 5(1)(c),

as excessive personal data may be collected.

- Different voice vendors may have different processes for improving upon their speech recognition models. One of these, as mentioned above, is the collection of users' biometric voice data for model training. Another process is audio review where humans carry out a manual review of an audio sample where a command was not actioned correctly. This enables the vendor to understand what went wrong and to manually improve their speech recognition model. The practice of audio review has not always been made clear to users of smart devices. Although vendors have worked to improve upon their transparency information and to allow individuals the option to opt out of this process, it is still something Novartis should take into account when carrying out due diligence of voice technology vendors.
- Although the accuracy of speech recognition technology has increased dramatically over the past few years, Novartis should enquire about the accuracy levels of models when carrying out its due diligence, in terms of the technology's ability to recognise different dialects, languages and genders. Flaws in the accuracy of the model may lead to inaccurate health data being collected by the solution, which in turn may lead to inappropriate clinical decision-making, or a solution that causes frustration to its users and is therefore not viable in practice.

4.15 The above risks should be considered in engagements with the voice technology vendors. Additional safeguards should be implemented into the design of the Digital Solution and measures should be agreed within contracts where necessary to minimise these risks.

Automated decision-making

4.16 Article 22 of the GDPR places restrictions upon organisations that carry out solely automated decision-making or profiling using personal data which may have a significant or legal effect on the individual to whom the data belongs. There are only very specific circumstances when a controller may carry out this type of processing. For example, where the decision is necessary for entry into or performance of a contract, where it is permitted by Union or Member State law, or where the individual has given their explicit consent to the processing. Under Article 22(4), automated decisions should not be based on

special category data unless the individual concerned has given their explicit consent or where the processing is necessary for reasons of substantial public interest. Even then, a controller must implement suitable measures to safeguard an individual's rights and freedoms and legitimate interests. An individual must also be given clear privacy information about the processing, should be able to challenge a decision, and be given the means to request human intervention.

- 4.17 With support from the Sandbox, from an early stage of engagement, a number of proposed use-cases were explored to identify whether any would involve automated decision-making without human intervention, and where this was the case whether the effect on an individual (the patient) could be considered as significant. For example, one potential use-case that was explored, involved automatically cancelling a patient's follow up appointment where the data presented a significant improvement in their condition based on the health assessment questions the individual had answered. It was discussed whether the patient's input into the questions could be considered as human intervention and also whether the cancelling of a routine follow up appointment would be classed as a 'significant effect'. It was agreed that for human intervention to be meaningful, it must come from a qualified clinician and not the patient themselves, and that automatically cancelling an appointment without this clinical input, could be deemed as a significant effect, therefore Article 22 would need to be considered. Article 22(4), also imposes additional restrictions where automated decisions are based on special category data. However, it was agreed that there was no appetite from a clinical perspective to use the solution to make fully automated decisions about patients or to replace clinical decision-making without necessary input from qualified health professionals.
- 4.18 As an alternative to the Digital Solution automating decisions fully, where it had identified from a pattern in the data acquired from the patient's responses to questions, that their condition had improved, the Digital Solution could provide an alert to the clinician that they should consider cancelling the patient's follow up appointment. As long as the clinician then examined the data for themselves and made their decision based on the available data rather than exclusively on the prompt from the Digital Solution, this would be considered meaningful human input.
- 4.19 An additional steer was provided to Novartis outlining some suitable safeguards to ensure that human input remains truly meaningful. When the solution is intended to be used by busy NHS clinicians, the risk of automation bias, where the clinician begins to rely on the Digital Solution's recommendations only, may be exacerbated. One safeguard may include appropriate

training of clinicians when the solution is implemented into a Trust, to ensure that they are aware of the risk of automation bias and that the solution should be used as a tool to support but not replace high quality clinical decision-making.

Communicating transparency information

- 4.20 Under Article 5(1)(a) and Articles 13 and 14 of the GDPR, data controllers have an obligation to communicate information about what they intend to do with an individual's data in a clear, concise and accessible way. This may be a challenge where a solution involves a number of components provided by different vendors, and to communicate complex processing entirely but in a clear and concise way.
- 4.21 As discussed, NHS Trusts where the Digital Solution is implemented will be the controllers, and these organisations will be responsible for providing privacy information to the users of the solution. However, Novartis has decided to develop privacy information itself for use within the user portals to support the NHS bodies with this obligation.
- 4.22 The vendor procured by Novartis to build the portal component to the solution has an existing privacy notice it uses when working directly with NHS bodies. The ICO and Novartis reviewed this privacy notice, and key points to this discussion were as follows.
- The use of ambiguous and vague language in privacy notices should be avoided. The information communicated to individuals should reflect the reality of the processing.
 - Information can be layered, including the most important information at the start, with more detailed information appearing later on in the privacy notice. Where there are different categories of data subjects, eg clinicians and patient users, information about the processing should be included under headings specific to that group of individuals. This is to avoid overwhelming other groups with irrelevant information not applicable to them.
 - Where a technology provider or processor decides to draft privacy information on the behalf of a controller for use within an application, some information about the controller and the purposes for processing should be included, and a

link to the controller's wider privacy notice should be signposted at the top of the document. Engagement with the controller will be required to ensure this information is accurate. The provider/processor can then go into more detail about how personal data is used specifically in terms of the solution.

- 4.23 A workshop was held to discuss the best ways to communicate the intricacies of speech/voice processing to end users. The use of smart devices and processing carried out by the large technology providers has been met with some public distrust previously. This is possibly due to a misunderstanding of the processing, and ambiguous or less transparent privacy information. These considerations included assessing the needs of vulnerable individuals and seeking input from individuals when designing transparency information. Where Novartis revisits the use of voice in the future, these considerations will be taken into account when drafting the privacy information.

5. Ending statement

- 5.1 Working with Novartis through the Sandbox, has allowed the ICO to build on its existing knowledge of complex business relationships and how technology providers may embed data protection by design into their products from early stages of development. Although providers may not always have a legal obligation to consider data protection, where the intention of a product is to process personal data on its deployment, all organisations within a supply chain should consider compliance within the design. This should not only ensure that the rights of individuals are considered from the early stages of product design, but it may also give providers an edge over organisations that have not thought about data protection, when competing for contracts, as controllers will be assured that they are meeting their obligations.
- 5.2 The Sandbox engagement also provided the ICO and Novartis, with valuable insight into the use of speech and voice data, in terms of the processing carried out by voice technology vendors in the consumer market and how the risks could translate into using voice technology in clinical settings. This is important as the use of smart devices and products which process user voice data, is likely to increase in the coming years. It is clear that understanding the intricacies of what the processing

of voice data entails is key to communicating clear transparency information to end users, which should in turn increase public trust of these products.

- 5.3 Through constructive and collaborative engagement with the ICO, Novartis gained new perspectives and insights into complex third party ecosystems, technological innovation, and emerging privacy challenges. In this context, Novartis was able to assess and manage third party risk, establish roles and responsibilities, and implement appropriate safeguards. Although it was determined that Novartis has no data protection role for the processing, and as such no direct legal responsibilities for personal data, Novartis followed the principles of accountability and data protection by design, to ensure requirements were identified and met.
- 5.4 The Sandbox also allowed Novartis to deepen its understanding of voice technology and the evolving risks in this area. Novartis will use this knowledge and the Sandbox steers when continuing its journey to design and deploy privacy-focussed voice solutions that can be used to support the NHS and improve patient care. Novartis will attempt to explore and participate in sandbox research and initiatives in countries that offer similar forms of constructive engagement.