Regulatory Sandbox Final Report: Our Future Health

A summary of Our Future Health's participation in the ICO's Regulatory Sandbox

Date: October 2023

Information Commissioner's Office

Contents

1. Introduction

1.1 The Regulatory Sandbox ('the Sandbox') is a service the ICO provides to support organisations that are developing products or services which intend to use personal data in innovative and safe ways, and will deliver a potential public benefit.

1.2 The Sandbox is a free, professional service that is available to organisations of all sizes who meet our entry criteria and specified areas of focus. We assess these criteria via our application processes.

1.3 The Sandbox specifically seeks projects operating within challenging areas of data protection. Sandbox participants have the opportunity to engage with us, draw upon our expertise and receive our support on mitigating risks and implementing data protection by design and default into their product or service. This helps ensure that the participant identifies and implements appropriate protections and safeguards.

1.4 'Our Future Health' is a private company limited by guarantee and a registered charity which operates within the health research sector. It is seeking to develop the UK's largest ever health research programme. Our Future Health aims to recruit a large cohort of individuals located in the UK, who will be demographically representative of the wider UK population, to participate in the research programme by voluntarily providing their personal data. Our Future Health intends to give external health researchers access to that dataset for use in health research. It hopes that this will provide health researchers with a unique opportunity to discover and test more effective ways to predict, detect and treat common diseases.

1.5 The ICO accepted Our Future Health into the Sandbox on 10 September 2021, determining that its project aligned with the ICO's data sharing area of focus at the time of its application.

1.6 The ICO and Our Future Health agreed to work on the following objectives as part of Our Future Health's bespoke Sandbox plan:

- **Objective one:** To consider the requirements under UK data protection legislation, taking best practice into

account, that Our Future Health will need, or may wish, to apply to its accreditation[1] criteria.

- **Objective two:** To consider the data protection roles and responsibilities of Our Future Health and its intended lawful bases for specific processing activities.
- **Objective three:** To consider how Our Future Health will approach the international transfer of personal data and whether Our Future Health's procedures in providing information to researchers mean that information is considered pseudonymised or anonymised under the UK General Data Protection Regulation (UK GDPR).
- **Objective four:** To assist Our Future Health in considering its documentation requirements, including how Our Future Health will provide transparency information.

1.7 The Sandbox work commenced in December 2021. The final objective of Our Future Health's plan was completed during January 2023. This report summarises the work that was carried out during its time in the Sandbox. It does not reflect the full detail of the discussions with, or the informal steers provided to, Our Future Health.

1.8 Some of Our Future Health's activities did not fall within the agreed scope of the Sandbox plan of work. For example, the Sandbox team did not carry out a review of Our Future Health's data protection impact assessment (DPIA). Our Future Health also stated it may seek to access other datasets such as NHS records or personal data held by devices such as wearable technologies and health or wellbeing applications. The combination, comparison or matching of any additional sources of personal data by Our Future Health, for example to contribute to the building of its database, was not within the scope of the Sandbox work. Our Future Health will need to ensure that all activities it carries out are fully compliant with UK data protection legislation.

[1] Our Future Health's 'accreditation criteria' should not be confused with the UK GDPR's requirements on certification which are established in Articles 42 and 43. This is explained further in section three of this report.

2. Product description

2.1 Our Future Health states that it is seeking to establish the UK's largest ever health research programme. It aims to produce better public health outcomes, such as people living longer and healthier lives, by helping to facilitate research into improving the prevention, early detection and treatment of diseases. Those diseases include conditions such as dementia, cancer, diabetes, heart disease and stroke.

2.2 To do this, Our Future Health intends to recruit a cohort of participants, from across the UK's different demographic groups, of up to five million people. This will be on a voluntary basis. It will ask the participants to provide a sample of their blood, which will be genetically analysed, alongside the answers to a detailed health and lifestyle questionnaire. This personal data will be stored in Our Future Health's primary data store (PDS).

2.3 Our Future Health's stated function is to allow health researchers access to that consolidated information via Trusted Research Environments (TRE) to carry out health research studies approved by Our Future Health. It hopes that this will inform discoveries about human health. Those researchers are likely to be affiliated with organisations such as:

- health bodies – eg the NHS;
- universities;
- charities; and
- companies involved in health research such as pharmaceutical companies.

Our Future Health hopes that combining the information it collects, and making it available for research, will allow these researchers to form a comprehensive understanding of what factors impact people's risk of disease.

2.4 Our Future Health acknowledges the importance of protecting participants' personal data and states in its Sandbox statement of participation that it is committed to protect their privacy. For example, Our Future Health states that it

will only provide access to its research programme to researchers working on research studies that have been approved by its 'Access Board'[2]. Additionally, Our Future Health will only allow access to personal data within TREs it has accredited. The ICO understands that as part of this accreditation process, Our Future Health has appointed a third-party assessor to conduct an assessment of the applicant's compliance with specific data protection and other requirements (for further information see commentary on 'Accreditation criteria' below starting in section 3.42). Our Future Health also states that it will only allow access to participants' personal data for the purposes of health research in the public good[3] and it will control what personal data is provided for each study.[4] Additionally, Our Future Health states that it will seek to pseudonymise its participants' personal data before it is made available to researchers in a TRE it has accredited. This process is discussed in more depth later in this report.

2.5 Our Future Health describes a TRE as a secure computing environment system where researchers' work is subject to clear rules, monitoring and controls. Its approach makes use of cloud infrastructure. Our Future Health will have its own TRE, run on servers in a UK public cloud. However, it states that its own TRE will not be able to meet the needs of every researcher. As a result it intends to allow external TREs, which have passed the TRE accreditation process developed by Our Future Health,[5] to host some of the data collected by Our Future Health as approved by its Access Board. Those external accredited TREs may be based outside of the UK. Our Future Health has indicated that it will seek to ensure both its own, and external TREs it accredits, apply the 'Five Safes Framework' developed by the Office for National Statistics.

[2] Our Future Health's Access Board is one of its Operational Boards that provide advice to the Board of Trustees and Executives, as well as making operational decisions. The Access Board is responsible for access to Our Future Health data, samples and participants.
[3] As a registered charity, Our Future Health states that it must meet the Charities Commission's criteria to demonstrate public benefit as an organisation. Our Future Health considers research to be in the 'public good' where it aims to improve the health of the general public and does not seek to promote health inequalities or stigmatise any particular social group.
[4] Our Future Health requires prospective researchers to complete a Study Application Form. As part of that researchers must identify, and justify, to Our Future Health what types of personal data they require access to in order to carry out their research.
[5] For the remainder of this report 'external accredited TRE' means an external TRE, distinct from Our Future Health, which has passed Our Future Health's accreditation process.

2.6 Our Future Health states that only registered researchers[6] will be able to access the personal data that Our Future Health makes available to them within an accredited TRE. The researchers must work with the personal data within the system and will be technically prohibited from removing it, as well as contractually prohibited from reidentifying it. It has also stated that the only information that researchers will be able to remove from an accredited TRE is the results of their research. Our Future Health will also use a manual output checking procedure to minimise the risk that an individual can be identified from anything exported from its own TRE (such as research results). The ICO also understands the TREs will contain analytical tools which researchers can use within the environment. This aims to avoid the need to remove personal data from the TRE.

2.7 Our Future Health has indicated that it will, in the future, contact participants to provide them with individualised feedback from the research conducted using their personal data or invite them to participate in additional studies. Participants will be asked to provide consent before receiving any feedback or participating in additional studies. This additional purpose was not within the scope of the Sandbox work and the ICO has not considered this future purpose as part of the Sandbox work. Our Future Health will need to carefully consider how it will comply with the UK GDPR's requirements before it commences processing personal data for this purpose.

3. Key data protection considerations

3.1 During its participation within the Sandbox, the ICO and Our Future Health considered a number of key data protection themes in relation to the development of the research programme under the objectives set out above. Some of those key areas of consideration are outlined below.

[6] Our Future Health defines a registered researcher as a person who has successfully completed the Our Future Health registration process and had their identity confirmed, including where necessary having had their bona fides (including their affiliation and qualifications) verified.

Data protection roles and responsibilities

3.2 It is crucial for any organisation seeking to comply with the UK GDPR to appropriately establish whether it is acting as a controller or processor for each processing activity it undertakes. Where more than one party is involved in the processing of personal data it is important to correctly establish the various data protection roles of those parties. This often requires a detailed assessment. Once established, all parties can then take appropriate steps to adhere to their various respective responsibilities under UK data protection law. During Sandbox participation, the ICO and Our Future Health worked together to consider what Our Future Health's data protection roles will be in relation to specified processing activities within its research programme.

3.3 Initially, Our Future Health proposed that, on the basis of its own assessment, it would be acting as an independent controller for most of the processing activities specifically discussed in the Sandbox. It also indicated that it had determined that the third-party controllers given access to the personal data (ie the registered researchers or the organisations to which they are affiliated) would also be independent controllers when they access personal data within Our Future Health's TRE, and within external accredited TREs, for most of the processing activities specifically discussed in the Sandbox. More information related to the status of personal data within the TRE is included later in this report.

3.4 In support of its assessment, Our Future Health stated for instance that its purpose is to make personal data available for registered researchers who will conduct health research separately to Our Future Health, and that it will only seek to facilitate that health research. Additionally, Our Future Health asserted that it will have no influence over the content of the proposals which researchers submit to access the personal data and, as a result, will not jointly influence the purposes and means of the processing. Our Future Health highlighted that it did not expect to benefit directly from the results of the research that is carried out on the basis of the personal data it held.

3.5 The ICO assisted Our Future Health in its assessment of its data protection roles and responsibilities by breaking down certain key processing activities to consider them in more granular detail. It should be noted that the support

provided by the ICO, and the content of this report, did not consider and do not detail a comprehensive list of all the processing activities that will be carried out within the research programme.

3.6 The ICO agreed that, for certain processing activities identified during Sandbox participation, Our Future Health will likely be an independent controller. For example, where Our Future Health collects personal data from participants via its questionnaires and samples, and stores that personal data in its PDS, it will likely be acting as an independent controller. The ICO also considered that Our Future Health will likely be an independent controller where it will seek to pseudonymise that personal data and transfer it to its TRE. In relation to these processing activities, the ICO understood that only Our Future Health will be involved in the processing of the personal data (ie only Our Future Health determines the purposes and means of the processing) and that was a key determining factor.

3.7 The key outcome of this work was identifying how the nature of controllership may change in relation to different processing activities. This is particularly relevant where personal data is processed in complex data sharing ecosystems that involve more than one organisation with differing levels of influence over the processing. For example, in relation to Our Future Health, registered researchers access personal data in Our Future Health's TRE to carry out health research and contribute results back into the TRE (such as reports, graphs, models and other research outputs) which may include personal data. In relation to these two processing activities the ICO noted that Our Future Health may be acting as a joint controller with the relevant third-party controller. Our Future Health has committed to reassess its position on joint controllership status when scoping the researcher contribution of results back to Our Future Health's TRE work.

3.8 In this context, the ICO encouraged Our Future Health to assess these activities in more detail to consider whether it is determining the purposes and means (the why and how) of the processing of personal data jointly with the relevant third-party controller (such as the organisations to which the researchers are affiliated). For example, the ICO encouraged Our Future Health to consider whether the intended processing activity would be possible without the participation of both Our Future Health and the relevant third-party controller. If Our Future Health concludes that the aims of each controller are inseparable, resulting in a common objective, and the processing would not be possible without both controllers it is likely that both Our Future Health and the relevant third-party controller(s) will be jointly

determining the purposes and means of the processing, and therefore acting as joint controllers. Joint controllership can also be established where controllers take separate, yet complementary, decisions about their own role in a processing activity, but they jointly influence why and how the overall processing operation works, without the need for any formal process of joint decision-making by the controller involved.

3.9 To help assess its processing activities further, the ICO identified factors for Our Future Health to consider that may indicate joint controllership and which specifically relate to its use case. The list below contains some example factors identified, but is not an exhaustive list of potential indicators of joint controllership that were discussed:

- Our Future Health's purpose in establishing the research programme and the research organisation's purpose in conducting an individual research study appear to be complementary and aligned.
- While the researchers will benefit from obtaining access to the TRE (allowing them to conduct research), it is also likely that their processing benefits Our Future Health's overarching objectives. Mutual benefit itself is not necessarily a decisive factor in establishing joint controllership, but it can be an indicative factor when considered alongside additional criteria.
- Our Future Health will determine the criteria of the application process that must be satisfied by the third-party controller in order for their research studies to be considered and approved by Our Future Health.
- Our Future Health's Access Board will determine which research studies will be granted access to the personal data within its TRE, thus enabling Our Future Health to influence the purposes for which such data can be processed.
- While the registered researchers elect to use Our Future Health's TRE and determine what personal data will be used within a particular research study, Our Future Health determines what personal data is originally collected and from whom. Our Future Health will also retain discretion over what personal data the researchers are granted access to.
- Researchers can only process personal data within the confines of the TRE and Our Future Health intends to

prevent the removal of any personal data from the TRE. Our Future Health remains operationally responsible for the security of the TRE, even whilst it is being accessed by researchers to process personal data (though the researchers remain subject to their respective security and accountability obligations under UK GDPR, if applicable).

3.10 The ICO's input was important to help Our Future Health assess how data protection roles and responsibilities can differ between processing activities. Where Our Future Health does act as a joint controller, the ICO reiterated what it means if you are a joint controller. This includes having a transparent arrangement in place to outline each joint controller's agreed responsibilities for complying with the UK GDPR and safeguarding individuals' personal data. Such an arrangement includes key requirements, such as the provision of transparency information and appropriately responding to individual rights requests.

3.11 It should be noted that this work focused on the data protection roles and responsibilities where personal data is processed in Our Future Health's own TRE. We have not considered the data protection roles and responsibilities of the various organisations involved where personal data is processed in an external TRE accredited by Our Future Health. It should also be noted that this section of the report details the steers the ICO provided to Our Future Health that identified factors relevant to its assessment of data protection roles and responsibilities based upon the information that was provided. Making that assessment remains the responsibility of the relevant controller(s).

3.12 Our Future Health's research programme involves the processing of personal data within a complex supply chain. Its work within the Sandbox will also help it assess controller and processor relationships with additional partners outside the scope of the Sandbox work. Those partners might include organisations such as the NHS, external TREs, IT providers (eg cloud software providers) and laboratories providing genetic analysis of samples.

Lawful basis for processing

3.13 Article 6 of the UK GDPR requires that a controller identify a valid lawful basis for processing in order to process personal data lawfully. Where that processing includes special category data, the controller must also identify an

appropriate condition for processing under Article 9 of the UK GDPR (and where necessary, an appropriate condition set out in Part 1 of Schedule 1 of the Data Protection Act 2018 (DPA 2018)). Which bases and conditions are appropriate depends on the purpose for processing personal data and the relationship with the individuals.

3.14 The ICO helped Our Future Health to further assess the lawful bases and conditions for processing identified by Our Future Health for specific processing activities which it intends to carry out. These activities are when Our Future Health collects and stores the participant's personal data in its PDS, where it pseudonymises that personal data and transfers it into its TRE, and where it makes the pseudonymised personal data accessible to registered researchers in Our Future Health's TRE in order for those researchers to carry out scientific research.

3.15 Initially, Our Future Health identified that it intended to rely upon consent, under Article 6(1)(a), and explicit consent, under Article 9(2)(a), to collect and store participants personal data in its PDS for subsequent use in health research. For the remaining purposes outlined in the above paragraph, Our Future Health indicated that it intended to rely upon legitimate interests, under Article 6(1)(f), and scientific research purposes, under Article 9(2)(j).

3.16 Based on the information provided during the Sandbox, the ICO considered that legitimate interests and scientific research purposes are likely to be the most appropriate lawful basis and condition for Our Future Health to rely on where it seeks to pseudonymise participants' personal data and then enter it into its TRE to be accessed by registered researchers. It is the responsibility of the controller to determine the appropriate lawful basis (and condition), and the ICO did not consider or confirm whether Our Future Health could discharge the relevant requirements for legitimate interests and scientific research in practice. Our Future Health must still satisfy the relevant requirements in full if it wishes to rely upon this lawful basis and condition. For example, the ICO did not review a full version of Our Future Health's legitimate interests assessment or assess the legitimate interests identified by Our Future Health. As a result, the ICO advised Our Future Health to ensure that it has appropriately assessed and documented whether the legitimate interests identified are not overridden by the interests, fundamental rights and freedoms of the data subject. The ICO has produced further information on how to apply legitimate interests in practice which is provided above. Where Our Future Health relies on scientific research purposes under Article 9, the ICO also noted that Our

Future Health must ensure that the processing is necessary, is in the public interest and that it has put in place appropriate safeguards (as per Article 89(1) of the UK GDPR and section 19 of the DPA 2018).

3.17 During this work, the ICO helped Our Future Health to reassess its intention to use consent and explicit consent where it collects and stores the personal data of research participants. Consent is not inherently better or more important than the alternative lawful bases and conditions under Articles 6 and 9 respectively. The ICO noted the high standard for consent under UK GDPR and the possible challenges in obtaining and maintaining valid consent in the circumstances, particularly in demonstrating that consent will always be freely given, specific, informed, an unambiguous indication of the data subject's actions, and withdrawable at any time. The ICO's research provisions guidance on consent also contains further considerations in relation to relying upon consent to process personal data for research purposes.

3.18 For example, the ICO highlighted to Our Future Health that, even at the first stage of processing (collection and storage), individuals will be providing their personal data to be used in health research. Whilst Our Future Health may be under separate legal or ethical obligations to obtain consent (separate to UK data protection requirements), such as consent from individuals to participate in health research in line with the common law duty of confidentiality, this should remain separate and not be confused with UK GDPR consent to process personal data. The ICO noted that UK GDPR consent is not necessarily required or appropriate just because there is a separate requirement to obtain consent or permission. There could be a risk that bundling various consents together may result in UK GDPR consent not being valid and individuals may be confused about what they are consenting to.

3.19 The ICO also highlighted to Our Future Health that for UK GDPR consent to be valid individuals must be able to withdraw their consent at any time. Our Future Health indicated that there are two ways in which a participant can withdraw from the Our Future Health research programme. They are partial and full withdrawal.[7] However, Our Future Health also advised that it will not be possible to remove a participant's personal data from any research carried out before the participant withdrew. As a result, the ICO noted that relying upon consent as the lawful basis or explicit

[7] Our Future Health describes its withdrawal processes further on its website.

consent as the condition for this processing activity risks merely giving the illusion of control – individuals would consent to the use of their personal data for research purposes, only for Our Future Health to be unable to fully provide for the participant's right to withdraw that consent.

3.20 The ICO hopes that, by carrying out this work, it has helped Our Future Health reassess its use of UK GDPR consent and explicit consent as its lawful basis and condition to process personal data for scientific research purposes. It also hopes that this has assisted Our Future Health to identify the most appropriate lawful basis and condition for this processing activity at the outset. The ICO suggested that Our Future Health conduct further work to assess whether legitimate interests and scientific research purposes are in practice an appropriate lawful basis and condition (respectively) for the purposes of the collection and storage of participants' personal data.

3.21 As a result of this work, Our Future Health has reassessed its lawful bases and conditions for processing personal data. It intends to rely on legitimate interests and scientific research purposes for all the processing activities outlined in section 3.14 of this report. The ICO hopes that this will help Our Future Health mitigate the risk of relying on an inappropriate lawful basis and condition, such as relying upon consent for processing activities where it is in fact not appropriate.

3.22 This work will also help Our Future Health to identify and mitigate risks in relation to its transparency and accountability obligations, for example confusion over how a participant's personal data will be processed and how they are able to exercise their individual rights.

Anonymisation and pseudonymisation

3.23 As part of the agreed Sandbox plan, the ICO and Our Future Health considered whether the information it will enter into its TRE will be pseudonymised, as per Article 4(5) of the UK GDPR, or anonymised considering the definition under Recital 26 of the UK GDPR. Pseudonymised data is still personal data and remains within the scope of the UK GDPR. The UK GDPR does not apply to anonymous data. This work focused on considering the status of the personal data in Our Future Health's hands. As part of this objective, the ICO and Our Future Health considered the ICO's draft

consultation guidance on anonymisation, pseudonymisation and privacy enhancing technologies to help inform this work. This draft guidance was published for consultation, which closed on 31 December 2022. It is subject to change following the consultation.

3.24 Our Future Health informed the ICO that it had concluded that the personal data in the TRE will be pseudonymous. This was because Our Future Health assessed that the personal data included within the TRE could, depending on the context, permit the indirect identification of data subjects. This means that Our Future Health could not guarantee that the data in the TRE would be anonymous in all scenarios. Our Future Health also stated that:

- it will be able to reverse the pseudonymisation process that it applies to the personal data before transfer to the TRE, and a limited number of staff would therefore be able to directly reidentify individuals for specific and necessary purposes;
- with their consent, it has the capacity to 'single out'[8] research participants so that various sources of their personal data may be linked together by Our Future Health using a pseudonym to create a richer picture of the research participant's health over long periods of time;
- it is not possible to anonymise genetic information whilst retaining its utility for research;
- it will be able to consider the research participant's risk of disease. Our Future Health may also, in the future, wish to provide feedback to participants related to their risk of disease, where that has been requested by the participant;[9] and
- it will retain the ability to reidentify research participants and may use that personal data to invite them to take

[8] Chapter two (How do we ensure anonymisation is effective?) of the ICO's draft consultation guidance on anonymisation, referenced earlier in this section, states that 'singling out' "…means that you are able to tell one individual from another individual in a dataset."
[9] This purpose of processing and future processing activity was outside the scope of the Sandbox.

part in additional research studies.[10]

3.25 As a result, Our Future Health confirmed to the ICO that it intends to treat all data within its TRE as personal data to ensure it is appropriately protected in accordance with the requirements of UK data protection legislation. It also stated that, by using pseudonymisation, it is seeking to protect the privacy of the research participants that take part in Our Future Health. As mentioned earlier in this report, some of the processing activities listed in the above bullet points (such as data linkage and considering an individual's risk of disease) were not considered within the scope of the Sandbox work. They are included here only to illustrate Our Future Health's own assessment of its processing activities, and the considerations that were taken into account in relation to this aspect of the work.

3.26 Based on the information provided as part of Sandbox participation, the ICO agreed with the assessment that it is likely that the personal data Our Future Health enters into the TRE will be pseudonymous (and not anonymous). The ICO considered that Our Future Health's ability to 'single out' individuals to carry out research in a longitudinal way, even if they cannot be identified by name, was a key factor. As it can reverse the pseudonymisation process, and reidentify participants, the personal data is not anonymous to Our Future Health.

3.27 This assessment assumes that Our Future Health will in fact pseudonymise the personal data (it is being processed in a way that meets the definition set out in Article 4(5) of the UK GDPR). The ICO reminded Our Future Health of the criteria for pseudonymisation outlined in Article 4(5) and Recital 26 UK GDPR, and the challenges of effective pseudonymisation. For example, the ICO noted that any additional information that can be used to attribute the data in the TRE to a specific individual, such as individual participant IDs in the PDS, must be kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Our Future Health has stated that it creates multiple participant IDs and uses a different set of IDs in the personal data that is transferred into the TREs than those in the PDS. It also states that the mappings between the IDs used in the PDS, and identifiers such as the participant's name, are kept separately. Our Future Health must also ensure that its pseudonymisation techniques are also sufficiently secure. This includes

[10] This purpose of processing and future processing activity was outside the scope of the Sandbox.

ensuring the algorithm is secure against malicious parties and third-party attacks. This is a risk that Our Future Health should assess as part of its DPIA.

3.28 As part of this work, the ICO also raised additional points for Our Future Health to consider. For example, Our Future Health will need to thoroughly assess the status of participants' genetic information that it will process to consider whether and how this information constitutes personal data and to ensure that it is processed in accordance with UK GDPR requirements.

3.29 The ICO did not assess, within the scope of the Sandbox work, whether the data in the TRE would be personal data in the hands of third parties. These third parties include external researchers approved by Our Future Health who access the TRE to carry out research. Each controller or processor accessing the TRE will separately need to comply with its respective obligations under UK data protection legislation where they process personal data. Chapter two of the draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies (published for consultation and referenced at the start of this section) contains information on assessing the risk of identifiability.

International transfers

3.30 Another key element of the Sandbox work was Our Future Health considering how it will approach the international transfer of personal data. This focused on the possibility of Our Future Health sharing personal data with external accredited TREs, located outside of the UK, to allow additional researchers to conduct health research, as described in section 2.5 of this report.

3.31 The UK GDPR primarily applies to controllers and processors located in the UK, with some exceptions. Where personal data is transferred outside of the UK, there is a risk that people will lose the protection of UK data protection legislation. As a result, the UK GDPR contains specific rules related to the transfer of personal data to separate receivers located outside of the UK, which are legally distinct from the sender. We refer to a transfer of personal data to these receivers located outside the UK as a 'restricted transfer'.

3.32 The first step is for an organisation to understand whether it is making a restricted transfer of personal data. What constitutes a 'restricted transfer' of personal data is described within ICO guidance via the link provided. The restricted transfer should also be necessary to achieve the organisation's aims – the sender should consider whether it can achieve its aims without actually sending the personal data.

3.33 Where a restricted transfer is necessary, in order to make a restricted transfer in accordance with UK GDPR, the sender must first consider whether it will be covered by adequacy regulations. UK adequacy regulations set out in law that the legal framework in a particular country, territory, or international organisation, or in a particular sector in a country or territory, has been assessed as providing 'adequate' protection for people's rights and freedoms about their personal data. The ICO guidance on international transfers identifies the countries or territories that are covered by adequacy regulations.

3.34 Where no adequacy regulations are in place the sender must assess if it can put in place appropriate safeguards to facilitate the restricted transfer (these are identified in Article 46 of the UK GDPR and detailed in ICO guidance). Our Future Health has stated it will be using international data transfer agreements. Before a sender can rely upon an appropriate safeguard, it must undertake a transfer risk assessment (TRA) to assess whether the safeguard provides the required level of protection. If the appropriate safeguard does not provide the required level of protection, the sender must undertake additional steps to ensure that the protections in the UK GDPR are not undermined for the data subjects whose data is transferred.

3.35 Where the restricted transfer is not covered by a UK adequacy regulation, and it is not reasonable or proportionate to put in place an appropriate safeguard, the sender must then consider on a case-by-case basis whether the restricted transfer may be covered by an exception identified in Article 49 of the UK GDPR. More detail related to these requirements is contained within the link at the start of this section of the report. The sender is unable to make the restricted transfer if there are no UK adequacy regulations covering the transfer, the sender is unable to implement and rely upon an appropriate safeguard, and there is no applicable exception in UK GDPR.

3.36 The ICO and Our Future Health worked together to understand the different ways in which a restricted transfer could occur within the research programme. For example, it was noted that it is possible that a restricted transfer could occur in the following ways:

- A restricted transfer from Our Future Health's UK based TRE to a separate recipient located outside of the UK, for example a registered researcher located outside of the UK accessing the personal data in the Our Future Health TRE.
- A restricted transfer from Our Future Health in the UK to an external accredited TRE, operated by another entity, located outside of the UK.
- An onward restricted transfer, of personal data received from the UK, from such an external accredited TRE located outside the UK to another entity, for example a registered researcher, located outside of the UK.

3.37 The ICO stated the importance in each scenario of understanding whether and when a restricted transfer is taking place, and which organisation is instigating the transfer. Whenever a restricted transfer takes place, Our Future Health must ensure it complies with the rules on restricted transfers, for example ensuring that an appropriate transfer mechanism is identified, documented and put in place. As a result of this work, Our Future Health acknowledged that it is possible that it will be initiating a restricted transfer by transferring personal data to an external accredited TRE located outside of the UK, or by providing access to registered researchers located outside the UK to its UK-based TRE (see paragraph 3.38 below). Where it is conducting a restricted transfer, it must take steps to comply with the UK GDPR's requirements on international transfers.

3.38 As indicated above, a key outcome of this work was that the ICO highlighted that restricted transfers may also be taking place within Our Future Health's own UK-based TRE. A restricted transfer can take place where personal data held in the UK is made accessible to a receiver outside the UK, such as via remote access. For example, a researcher who works for a university located outside the UK might access Our Future Health's UK-based TRE to conduct research into treatments for a particular condition. As the non-UK university will be processing the personal data, a

restricted transfer may be taking place. This is because the university, which is a legally distinct controller, is accessing personal data held by Our Future Health in the UK.

3.39 As a result, the ICO has highlighted to Our Future Health that making personal data accessible to registered researchers may constitute a restricted transfer of personal data. Where it does, Our Future Health must ensure that the applicable restricted transfer rules are complied with.

3.40 Our Future Health also posed a number of questions to the ICO in relation to the factors that would affect Our Future Health's assessment as to whether a restricted transfer is taking place. For example, the ICO and Our Future Health discussed the importance of where a recipient organisation is based and the location of its servers, and whether the personal data will be processed by a legally-distinct recipient. These facts will need to be established by Our Future Health and requires thorough understanding of its personal data flows. The ICO noted that the nationality of a registered researcher will not constitute a relevant factor in whether a restricted transfer is taking place, and that an IP address only indicates the location of a user's internet connection and therefore does not necessarily indicate a user's physical location in practice.

3.41 In addressing Our Future Health's questions on restricted transfers, the ICO maintains that Our Future Health will need to consider each potential restricted transfer, on a case-by-case basis, considering the requirements under UK data protection law. The ICO's guidance, linked to in section 3.30 details those requirements in more depth. The ICO emphasised that Our Future Health must ensure that it has comprehensively assessed and mitigated any risks to individuals caused by the international transfer of their personal data within its DPIA and TRAs, and that it has provided appropriate transparency information in relation to international transfers.

Accreditation criteria

3.42 Our Future Health has developed a set of internal 'TRE accreditation criteria' which it intends to use to assess, approve and audit the wider practices, policies and procedures of its own and external TREs. The accreditation criteria cover a wide range of topics, including the requirements of UK data protection legislation. The ICO reviewed the

specific criteria relating to UK data protection requirements as part of the Sandbox process. This report does not comprehensively list all of the feedback provided by the ICO to Our Future Health in relation to these criteria.

3.43 The UK GDPR does not specifically require the development of accreditation criteria for controllers to use internally for audit purposes, or for the purposes of conducting due diligence on third parties prior to sharing personal data. However, the UK GDPR contains accountability obligations, which apply generally to the sharing of personal data and the ICO data sharing code of practice contains further information about sharing personal data in a way that complies with UK data protection law. During its Sandbox participation, Our Future Health indicated that it has voluntarily decided to use this mechanism as part of its approach to data protection by design and default when sharing its participants' personal data.

3.44 The ICO understands that Our Future Health's accreditation criteria will be used by a third-party assessor, appointed by Our Future Health, as part of its internal audit and external due diligence process when providing its own and external accredited TREs with access to personal data. From a high-level perspective, the ICO considered that this process could in theory provide a helpful mechanism as part of a wider effort by Our Future Health to comply with its data protection obligations, such as in relation to accountability, purpose limitation and data minimisation. However, the ICO cautioned that if Our Future Health is to rely on such an approach, it must ensure that its criteria are consistent with the requirements set out in the UK GDPR. The ICO also recommended that the accreditation process is sufficiently resourced, in order to operate efficiently, and is regularly reviewed and updated where appropriate to ensure the accreditation criteria are effective. Our Future Health has since stated that these actions are complete.

3.45 The ICO also suggested to Our Future Health that it may wish to consider developing a certification scheme, under Article 42 of the UK GDPR, for the processing activities it is seeking to accredit. The benefits of certification schemes can include enhanced transparency, improved business to business and public relationships and trust, improved accountability and the establishment of best practice standards. However, the development of a certification scheme is voluntary and is not required by the UK GDPR.

3.46 In relation to individual rights, established by Articles 12 to 23 of the UK GDPR, the ICO helped Our Future Health to ensure that its accreditation criteria reflect that any policies or processes that are implemented recognise that data

subject requests should be assessed on their individual merits. This is particularly relevant given the context of the processing within the research programme and the exemptions from individual rights in relation to research under the UK GDPR. Additionally, given the observations around joint controllership (as summarised earlier in this report), the ICO noted that if Our Future Health acts as a joint controller it must be clear about who is responsible in practice for replying to individual rights requests, and that individuals are informed and clear about this via appropriate transparency information. The ICO informed Our Future Health that its accreditation criteria, in relation to individual rights, should reflect this consistently. The ICO reiterated that a joint controllership relationship requires a transparent arrangement in place with each fellow joint controller in accordance with Article 26 of the UK GDPR, which must set out how each joint controller will deal with data subject rights. Though joint controllers may specify a central point of contact for individuals, and assign operational responsibility, individuals must still be able to exercise their rights against each controller.

3.47 Our Future Health's TRE accreditation criteria also included a requirement for an external TRE to evidence that it had completed a DPIA, where required by the UK GDPR. The ICO stated that even where a DPIA is not specifically required it can be good practice to complete one. Whilst an external organisation is not obliged under the UK GDPR to share its DPIA with Our Future Health, the ICO recommended that Our Future Health ensures it is clear as to what information it is seeking both for its internal DPIA and from external organisations and why. For example, the ICO encouraged Our Future Health to consider what kind of risks and mitigations it would require as part of its assessment process. Our Future Health's criteria should also clearly reflect prior consultation requirements. Our Future Health has stated that it has decided that external TREs will only be required to submit a template DPIA to Our Future Health as part of its TRE accreditation process.

4. Ending statement

4.1 Given the scope, proposed scale and sensitivity of Our Future Health's intended processing of personal data, this was a complex Sandbox project. The work gave both the ICO and Our Future Health further insight into how a data protection by design and default approach can be implemented within an intricate health research environment. As

Our Future Health expects to recruit a significant number of research participants, these learnings are likely to be important as it seeks to protect the data protection rights of its participants.

4.2 Following the completion of its Sandbox participation Our Future Health stated the following: "Our Future Health's participation in the Sandbox demonstrates to the public a commitment to data protection by design and default and to implementing data protection best practice across every aspect of the programme. Its commitment to protecting the privacy of research participants has been supplemented and strengthened by the ICO's expertise and steers. Of particular benefit were discussions around lawful basis, controllership, international data transfers and the development of the TRE accreditation process. It was particularly important to engage with the ICO at the start of the programme, which will run for many years into the future, to ensure best practices are embedded proactively. The impact of this work will be felt by all programme participants and researchers engaging with Our Future Health over the years."

4.3 The health research sector, and public health generally, has been subject to increasing public interest and attention in recent years. This Sandbox project has helped to highlight the importance of ensuring data protection by default and design when building and implementing health research programmes from the outset. The ICO and Our Future Health worked together positively throughout the project, which demonstrates the ICO's role as a trusted information rights regulator, and the practical benefits of participating in the Sandbox. The ICO hopes that participation has been beneficial to the development of Our Future Health's research programme and its aim to benefit wider public health outcomes. This project underlines that compliance with data protection legislation is not a barrier to innovation.