Our Future Health

Trusted research environment accreditation policy

Version 1.2 June 2022

Our Future Health

Trusted research environment accreditation policy

1. Introduction

Our Future Health will make data available for research within trusted research environments (TREs), a type of secure data environment. This is in line with the latest policy developments, for example the NHS Data Saves Lives strategy.

TREs offer a highly secure computing environment, where researchers can access and work with data subject to rules and monitoring, but which have very strict controls on what data they can take away. The controls limit what data can be removed, to minimise the risk that an individual can be identified. Taking this approach will help to build public confidence that health data is being accessed securely, used appropriately and that people's privacy is being protected.

The Our Future Health trusted research environment will be the default way for most researchers to study the data. We are working closely with researchers to ensure it is useful for the widest possible range of users, and meets the diverse needs of the community. Our TRE aims to both speed up research, and to maximise the value and potential impact of discoveries on prevention, early detection and treatment of major diseases. There could also be occasions where the Our Future Health TRE may not be able to meet certain specific research requirements. So, where other TREs can meet the same strict standards as the Our Future Health TRE, we will allow other TREs to host the consented, de-identified Our Future Health data to run approved research projects.

We have an accreditation process that is designed to ensure that a trusted research environment hosting Our Future Health data meets the necessary standards of data governance and cyber security, as well as operational, privacy and technical requirements to receive Our Future Health data. This is based on existing, well-established standards and frameworks, such as the Office for National Statistics Five Safes framework, the UK GDPR, and international cyber security standard ISO 27001. A TRE must successfully complete this process and achieve accreditation before it can receive Our Future Health data. All research projects must also be approved by our Access Board.

2. Scope

This document outlines our approach to the accreditation of trusted research environments. It is separate from the NHS England secure data environment accreditation process, referenced in the Data Saves Lives strategy.

This document covers:

- Our Future Health accreditation rules
- Documentation relating to the Our Future Health accreditation process

This document does not cover:

- Researcher registration process
- Access process
- Data transfer to TREs
- Data sharing agreements
- Details about the Our Future Health TRE

3. Definitions

Access Board: Our Future Health board responsible for developing and implementing the access process, and authorising decisions about research applications to access the Our Future Health resource.

Access process: the process by which all research studies using the Our Future Health resource are approved. Includes decisions about access to data and datasets. Our Future Health is responsible for this process, which is overseen by the Access Board.

Accreditation: the process developed by Our Future Health to ensure a TRE has demonstrated sufficiently robust organisational, technical, security and administrative processes to be permitted to host a subset of the Our Future Health data to allow registered researchers to conduct an approved study. Accreditation is granted by an independent assessor to a specific TRE.

Approved study: a study or research project approved by the access board. The studies are approved for a fixed period of time.

Applicant: an organisation with a TRE that applies for accreditation of that TRE via the Our Future Health accreditation process.

Assessor: third party commissioned by Our Future Health to review accreditation applications, including the self-assessment questionnaire and evidence.

Data Protection Officer (DPO): a data protection officer ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organisation are described in Articles 37, 38 and 39 of the UK General Data Protection Regulation.

Pseudonymised data: personal data that has been processed in such a way that the personal data can no longer be attributed to a specific person without the use of additional information. Pseudonymisation is a method of data de-identification.

Registered researcher: a person who has successfully completed the registration process and had their identity confirmed, including where necessary having had their bona fides (including their affiliation and qualifications) verified.

Resource: the Our Future Health data and samples; the Our Future Health TRE; the results data from any approved research project that is added to the Our Future Health TRE; and a register of plain English summaries of each approved study.

Standard Operating Procedure (SOP): a set of written instructions that describes the step-by-step process that must be taken to properly perform an activity.

Trusted research environment (TRE): is an environment that allows registered researchers working on an approved study to conduct analysis on the Our Future Health pseudonymised datasets in a secure manner.

UK General Data Protection Regulation (UK GDPR): the UK's domestic data privacy law, which took effect on 31st January 2020. The UK's implementation of the EU GDPR.

4. Accreditation

the following guidelines underpin the Our Future Health process.

4.1.1 Our Future Health aims to ensure the accreditation is fair, transparent, and not unnecessarily burdensome.

4.1.2 The accreditation process will ensure an organisation hosting Our Future Health data has robust technical, cyber security, operational, and administrative controls.

4.1.3 The accreditation will re-use existing standards and frameworks as much as possible.

The accreditation is based on:

a. UK GDPR, including Transfer Impact Assessment for international transfer of data
b. ISO 27001 Annex A
c. Caldicott principles
d. Common Law of Confidentiality
e. Our Future Health Ethical Framework and Protocol
f. NHS Data Saves Lives strategy
g. UK Health Data Research Alliance Paper "Principles and Best Practices for Trusted Research Environments"
h. Five Safes Framework

4.1.4 The accreditation will apply equally to all TREs seeking to host Our Future Health data.

4.1.5 Our Future Health, organisations with TREs accredited by Our Future Health, and the registered researchers who are conducting approved studies will be classed as independent data controllers. The accreditation has been designed for this arrangement.

4.1.6 The scope of accreditation includes the TRE and all associated processes, including data import and data export processes.

4.1.7 Our Future Health will publish a list of projects approved by the Access Board, including information on where the project is taking place, i.e. in which accredited TRE the research will be.

4.1.8 The accreditation assessment will be carried out by a third-party assessor, using a scoring framework.

4.1.9 Our Future Health data will be protected using the 5 Safes model, originally developed by the Office for National Statistics.

a. Safe People: Only trained and registered researchers will access the data within a Trusted Research Environment. Researcher credentials, experience, and training in data governance and safe data handling processes will be checked by the Our Future Health researcher registration process.
b. Safe Projects: Data will only be used for ethical, approved projects with a clear public health benefit. All projects and applications to access data will be reviewed and approved by the Our Future Health Access Board.
c. Safe Settings: Any Trusted Research Environment hosting Our Future Health data will have strict technical, administrative, operational, and security controls which manage and monitor all aspects of how it works, and how users interact with it. This will be checked via the Our Future Health accreditation process.
d. Safe Data: All Our Future Health data in a Trusted Research Environments will be pseudonymised to protect the privacy of participants. Additionally, use of the data within the Trusted Research Environment will be logged, a requirement of Our Future Health accreditation.
e. Safe Outputs: Strict technical and security controls, as well as operational and governance processes, will be checked via the Our Future Health accreditation process and will determine what data can leave the Trusted Research Environment. This is to minimise the risk of data that can identify an individual participant leaving the environment. These include strict data export rules agreed to as part of a legally binding contract and independent auditing of data exports.

4.1.10 The accreditation assessment is grouped under sixteen overarching accreditation principles, which assess operational, data governance, and cyber security requirements. See the accreditation self-assessment questionnaire for further details.

4.1.11 Accreditation and the international transfer of data will be subject to UK GDPR rules, and where relevant a Transfer Impact Assessment.

4.1.12 An organisation with a TRE accredited by Our Future Health will be subject to the following measures:

a. Contractual arrangements and responsibilities
b. Data sharing agreements
c. Annual review of: changes; security incidents; researcher access; ongoing studies; threats; data exports; data deletion; and other processes. Some of these items will also be reviewed on an immediate or more regular basis
d. Re-accreditation of changes
e. Incident management and security reporting procedures
f. Audit as required by data controllers
g. Re-accreditation as required by changes to the Our Future Health accreditation process

4.1.13 A fee for accreditation and ongoing maintenance of accreditation will be charged by Our Future Health.

4.2 At all times, Our Future Health data may only be stored and accessed:

f. Within a project specific workspace within an accredited TRE
g. By a registered researcher
h. As part of a study approved by the Access Board
i. For the purpose approved by the Access Board
j. For the duration allowed by the Access Board

The Our Future Health data may not be linked to additional data relating to Our Future Health participants which may be available to a TRE user, apart from as part of an approved research project that involves recontacting participants and securing their consent for the linkage.

4.3 Our Future Health data will never move between TREs. Data will only flow from the Our Future Health primary data store into an accredited TRE as approved by the Access Board.

4.4 Our Future Health data will only be transferred to an accredited TRE as allowed by data controllership rules, data sharing agreements, and data licensing agreements.

4.5 The Our Future Health data held within a TRE is classed as pseudonymised data, which is treated as personal data for the purposes of UK GDPR. The only Our Future Health data that may be stored in a TRE is pseudonymised data.

4.3 Example reasons for use of an external accredited TRE:

Organisations may want to apply for the accreditation of their TRE in order to use data, software or hardware which are difficult, infeasible, or impossible to replicate in the Our Future Health TRE. These examples are not exhaustive.

Example 1 – data: Multiple large-scale genetic, clinical and epidemiological datasets are increasingly being used together to enable deeper insights into human health and disease. Researchers may wish to access Our Future Health data for joint analysis with existing large collections of data from other studies to enable maximal insights in data analytics. Bringing these additional datasets into the Our Future Health TRE may be infeasible or impossible due to complex data structures or content, dataset size meaning transfer is not possible, or legal agreements restricting their distribution. An accredited TRE would make it possible to bring the Our Future Health datasets to existing data, enabling a larger variety of research as well as providing deeper insights into the detection and prevention of disease.

Example 2 - software: Organisations have developed complex analysis pipelines for genetic and image data with a range of specific dependencies that the Our Future Health TRE may be unable to meet (because they exist on different systems, are obsolete, proprietary, etc.). It may only be feasible to deploy these pipelines, and conduct the specific analyses which use them, in an accredited TRE.

Example 3 - hardware: Novel methods in machine learning are often enabled by developments in the computational capabilities of computing hardware, especially processors. With the scale of genetic data in the terabytes to petabytes, novel deep learning methods might initially only be feasible with specialised AI accelerator hardware that may not be available on the Our Future Health TRE.

5. Documentation

5.1 Our Future Health accreditation documentation.

	Document	Status
1	Accreditation policy	Published
2	Accreditation self-assessment questionnaire	Published
3	Accreditation of a TRE SOP	Published
4	Change to an accredited TRE SOP	Published
5	Updating accreditation SOP	Published
6	Account management of an accredited TRE SOP	Published
7	Withdrawal of accreditation SOP	Published
8	Data deletion SOP	Available autumn 2022
9	Statistical disclosure control SOP	Available autumn 2022
10	Incident management SOP	Available autumn 2022

5.1.1 Accreditation policy

This document, outlining Our Future Health's approach to the accreditation and ongoing maintenance of accredited TREs.

5.1.2 Accreditation self-assessment questionnaire

A self-assessment questionnaire structured around 16 accreditation principles, to be filled in by applicants. Self-assessment answers plus supporting evidence will be reviewed by an independent assessor.

5.1.3 Accreditation of a TRE standard operating procedure

A standard operating procedure describing the process by which organisations apply for accreditation of their TRE by Our Future Health.

5.1.4 Change to an accredited TRE standard operating procedure

A standard operating procedure describing how changes to elements of the systems and processes related to an accredited are reviewed and/or reaccredited.

5.1.5 Updating accreditation standard operating procedure

A standard operating procedure describing the process by which Our Future Health may make updates to the accreditation materials or processes.

5.1.6 Account management of an accredited TRE standard operating procedure

A standard operating procedure describing the process for: the ongoing maintenance of the accreditation; the review of the systems, processes and risks; and account management topics; at a minimum every 12 months.

5.1.7 Withdrawal of accreditation standard operating procedure

A standard operating procedure describing an objective process for withdrawal of accreditation from an accredited TRE in limited circumstances, based on remediation and review by a third-party assessor.

5.1.8 Data deletion standard operating procedure

A standard operating procedure describing the requirements for data deletion and archiving of Our Future Health data within an accredited TRE.

5.1.9 Statistical disclosure control standard operating procedure

A standard operating procedure describing the process by which it is ensured no individual is identifiable from results data, for the purpose of protecting the confidentiality of the research participants.

5.1.10 Incident management standard operating procedure

A standard operating procedure describing the requirements for security incident management and reporting.