Administrative Data Research Network

An ESRC Data Investment

Trusted Third Party Policy

PUBLIC

01 JULY 2015

Version: 01.00

T +44 (0)1206 873435
E help@adrn.ac.uk
www.adrn.uk

Scope

In order to support ADRN's commitment to protect the privacy and confidentiality of data subjects a suite of Information Assurance policy documents have been developed to provide a framework for ADRN operations and to guide practice across all ADRCs and the ADS. This document outlines the ADRN policy in relation to a Trusted Third Party. All ADRCs will in addition have local procedures that outline how these policies are operationalised.

Other associated documents include:

ADRN030 Privacy Protection and Information Security Principles

ADRN032 Secure Environments Policy

ADRN033 Data Movement Policy

ADRN034 Data Retention and Destruction Policy

Trusted third party (TTP)

A Trusted Third Party (TTP) is an organisation that performs the matching of direct identifiers from different data sources.

The Trusted Third Party (TTP) fulfils a vital role in ensuring the privacy of research subjects. TTPs enable the ADRN to ensure that the data that can identify an individual is never held by the same entity that holds the analytical information (e.g. de-identified payload data or research data). The TTP receives identifying information from which it creates an anonymous index that matches the IDs of the two datasets (which are then deleted). The index is then used by an ADRC to link the datasets anonymously to produce a de-identified research dataset.

Contents

For defintions of terms please see the ADRN glossary at http://www.adrn.ac.uk/using-the-network/documentation

1. TTP Policy

This policy sets out the standards and requirements for parties who provide a Trusted Third Party service to ADRN, and is arranged according to the ADRN Principles that the policies underpin. Each ADRC is required to ensure that all TTPs providing a service to them comply with this policy.

ADRN1: ADRN will always operate to protect the privacy and confidentiality of data subjects.

1. TTPs must agree to abide by ADRN applicable policies and procedures.
2. TTP physical environments and processes must be accredited by CLAS [CESG[1] Listed Advisor Scheme] consultants. TTPs must comply with external audits as commissioned by the ADRN.
3. TTPs will only ever transfer data to an ADRC or originating data controller. All data transfers must be secure and compliant with ADRN033 Data Movement Policy.
4. For each research project the TTP will be provided with a clear specification regarding

[1] CESG is the Information Security arm of GCHQ. CESG protects the vital interests of the UK by providing advice and guidance to the UK government on the security of communications and electronic data, in partnership with industry and academia. http://www.cesg.gov.uk/Pages/homepage.aspx

data requirements, including metadata such as a project/linkage proposal.

5. TTPs will have data processing agreements with data controllers in place for all data they receive and process.

6. TTP will only act as requested in the project specification, and the data processing agreement.

7. TTPs must notify the ADRC that is responsible for the approved project for which the data are being created and the data controllers if data or information are received that are not in the project specification.

8. TTPs will generate project specific matched index numbers in line with CESG's specification. TTPs will follow the requirements of the ADRC that is responsible for the approved project for which the data are being created in relation to the treatment of unmatched data, which will be in accordance with the project specification.

9. Any organisation within ADRN that is undertaking multiple roles of data controller, TTP and/or ADRC, must have an explicit separation between the functions.

   This must include separation of staff, projects and direct management responsibility, and a separation of all IT facilities either physically or virtually.

10. TTPs are not required to create 'derived variables' from two or more datasets. To ensure the 'separation of function' principle is maintained derived variables will be created within ADRCs.

11. During the matching process, TTPs will not communicate directly with either data controllers or researchers. All communications will be via the ADRC that is responsible for the specific approved research project.

ADRN4: ADRN will ensure data are accessed safely and securely.

12. TTPs may be asked to actively participate in the development stage of a project application.

ADRN5: ADRN will be accountable and operate under appropriate governance.

13. TTP will operate under a written agreement between one or more ADRCs and the TTP.

14. TTPs are expected to have a major incident protocol related to data security and privacy breaches and must provide evidence of this to the ADRC they are working with.

15. A list of Trusted Third Parties used by the ADRN will be available on the web site.

16. A summary report, including match rates will be prepared by the TTP and sent the ADRC on completion of the matching process.