Administrative Data
Research Network

An ESRC Data
Investment

Privacy Protection and Information Security

Guiding principles

PUBLIC

01 JULY 2015

Version: 01.00

T +44 (0)1206 873435

E help@adrn.ac.uk

www.adrn.uk

Scope

This document outlines the Administrative Data Research Network's (ADRN) information security principles. Information security and the safe-guarding of personal identities (whether these are individuals, households, businesses or other organisations) is a key ADRN commitment. These principles provide a foundation for the safe processing of de-identified, administrative data that are to be accessed for the purposes of research that will benefit the UK public.

These principles inform the ADRN information security policies:

ADRN031 Trusted Third Party Policy

ADRN032 Secure Environments Policy

ADRN033 Data Movement Policy

ADRN034 Data Retention and Destruction Policy

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

1.   Introduction

Scientifically sound and ethically robust research is an essential part of protecting and improving public services. Administrative data can give us an in-depth and accurate picture of society which is extremely valuable for social and economic research. The findings have the potential to significantly influence future government policy and how politicians and others evaluate existing policies. For more information on ADRN and the benefit of using administrative data for research, please see our website http://www.adrn.ac.uk/admin-data/benefits.

The Administrative Data Research Network (ADRN) is a UK-wide partnership between universities, government departments and agencies, national statistics authorities, the third sector, funders and researchers. We help accredited researchers carry out social and economic research using linked, de-identified administrative data – information which is routinely collected by government organisations.

ADRN is strongly committed to abiding by a set of overarching principles, of which the following apply directly to Information Security:

> ADRN1: ADRN will always operate to protect the privacy and confidentiality of data subjects.
> ADRN4: ADRN will ensure data are accessed safely and securely.
> ADRN5: ADRN will be accountable and operate under appropriate governance.
> ADRN10: These overarching principles must guide all ADRN practice across all ADRCs and the ADS, and key policy documents will also be network-wide. Where implementation of policies must vary, due to differences in local infrastructures or different legal frameworks among the devolved administrations, these will be fully documented in local procedural documentation, and will at all times adhere to these overarching principles.

The principles and standards presented here are designed to underpin ADRN's core principles and to ensure that Administrative Data Research Centres (ADRCs) operate effectively and to equivalent standards when managing the risks inherent in any data sharing, linkage and analysis. In line with the ADRN principles above, where implementation of policies must vary, due to differences in local infrastructures or different legal frameworks among the devolved administrations, these will be fully documented in local procedural documentation.

2.   Principles

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

1. ADRN will comply with legal guidelines and current legislation.

2. ADRN will keep abreast of and comply with best practice guidelines on information security.

3. ADRN will ensure that all staff have appropriate, and up to date, training in Information Governance and the law relating to the protection of individuals' privacy.

4. No research outputs will be released from the ADRN without the application of disclosure control to minimise the risk of re-identification.

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

5. All data movements within the ADRN will be undertaken securely and individuals' privacy protected.

6. ADRN only provides access to de-identified data for ADRN Accredited Researchers with Approved Projects.

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

7. ADRCs will only process data on behalf of the data controllers; they will not be data controllers in their own right.

8. ADRN will be transparent about data retention and destruction. [see ADRN034 Data Retention and Destruction Policy]

9. All data will be held and processed securely within the UK.

10. ADRN is committed to continual improvement in our processes and procedures and will continue to develop our information security procedures throughout the life cycle of the ADRN.