Use of NHS Central Register Data in the Scottish Longitudinal Study
Report on privacy safeguards

A report by National Records of Scotland

Published on 29 October 2013

Contents

1. Overview

The Scottish Longitudinal Study (SLS) is a 5.5%[1] representative sample of the Scottish population, which is selected using 20 semi-random dates of birth occurring in any year.

People whose records are stored in the SLS are referred in this paper as SLS members.

The SLS includes sensitive personal information from SLS members (and some information about their direct relatives) collected from:

- Census (1991 and 2001).
- Vital Events: births, stillbirths, deaths and marriage of SLS members, and also infant mortality and widow(er)hoods when the SLS member is the relative of the deceased.
- NHS Central Register (NHSCR) data (migration in and out of Scotland).
- Cancer registrations and hospital discharges from NHS record. This information is not stored in the SLS but obtained when requested for specific studies through a complex linking process.
- School census, Scottish Qualifications Authority (SQA) attainment and information on school absences/exclusions.

This collection of records allows comparing the individual's changing circumstances over time.

The NHS Central Register Governance Board commissioned National Records of Scotland (NRS) to prepare a report which addresses:

- privacy issues in relation to the transfer and use of data from the NHS Central Register in the SLS; and
- safeguards in place to protect personal information.

This is a summary of the full report. It is not possible to publish the full report as it contains potentially disclosive material.

2. The Scottish Longitudinal Study (SLS) – The Process

The SLS is a dynamic dataset which is continually updated. Any persons born on SLS dates are included in the sample if they were either born in Scotland or have migrated into Scotland from elsewhere between the 1991 and 2001 Censuses. Exits from the study are either by death or emigration and re-entries can occur into the study if emigrants return to Scotland.

The NHS Central Register (NHSCR) database is vital to SLS as it is the only database that includes the majority of the British population from birth. All SLS members are flagged in the NHSCR with a unique study number which allows the linkage of data to be done without compromising confidentiality.

Footnote

1) Although it has only achieved a 5.3% sample of the population of Scotland.

3. Data Protection Act (DPA) 1998

National Records of Scotland (NRS) complies with the eight principles in the Data Protection Act 1998 ('DPA'). This section covers the main DPA issues that affect the use of the NHSCR in the Scottish Longitudinal Study (SLS).

Information about the use of NHSCR data in the SLS is provided to data subjects on the NHSCR section of the NRS website.

Consent

The birth dates for SLS subjects are secret so it is not possible to obtain consent for the use of their personal information. An alternative conditions for processing in the DPA are relied upon, being **Schedule 2 Condition 6** ('the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject').

No 'sensitive personal data' is stored in the SLS. When highly sensitive data such as NHS cancer data, maternity data and hospital admissions data is required for an SLS project, the approval of the NHS Services Scotland Privacy Advisory Committee (PAC) is needed.

Data Protection Act research exemption

The use of NHSCR data in the SLS qualifies for the research exemption because it fulfils the following 'relevant criteria':

(a) the data are not processed to support measures or decisions with respect to particular individuals and

(b) the data are not processed in such away that substantial damage or distress is or is likely to be, caused to any data subject.

NRS's compliance with the DPA research exemption means:

- the processing of NHSCR data as part of the SLS complies with the DPA even though it was not the original purpose for which the data was collected;
- the data may be kept indefinitely; and
- NRS are exempt from complying with the subject access provisions of the DPA (because NRS fulfils the additional criteria that results of research do not identify any individual).

4. Confidentiality

The following legislation and guidelines cover the Scottish Longitudinal Study (SLS) data use and data release:

- National Statistics Code of Practice and, in particular, the Protocol on Data Access and Confidentiality;
- the Census Act 1920;
- the Population (Statistics) Act 1938;
- the Data Protection Act 1998; and
- the Freedom of Information legislation.

A series of controls are in place for National Records of Scotland (NRS) staff to ensure confidentiality:

- Only a small group of researchers are aware of the birth dates for SLS members.
- SLS members' names and address are not included in the SLS dataset.
- The method of linking Census and Vital Events maintains the anonymity of the SLS members.
- SLS records available for analysis are anonymised individual-level data.
- SLS dataset is held at the NRS secured building. It can be accessed only from a secured room using password protected computers not connected to any network.
- The only aggregated data outputs that can be sent to SLS users out with the secure room are tabulations and model outcomes (such as regression coefficients). Outputs are always sent encrypted and are not disclosive.

Researchers working with SLS data must read and sign a Disclosure Control Policy, the 2001 and 2011 Census Confidentiality guidelines and other documents for confidentiality.

Raw microdata files are not provided to anybody. Instead, two options for accessing SLS data are available:

- Remote access: a researcher submits syntax to the SLS team to run on their behalf. Both the code and the output data is checked for disclosure and to avoid the detection of a single individual. Researchers submissions may be returned for corrections after those checks and re-run when corrected.
- A safe haven based in the NRS in Edinburgh can be physically accessed by researchers under strict rules, after contacting the SLS Support Team. Once a researcher contacts the SLS Support Team:
  - The research proposal is reviewed by the SLS Support Team and the PAC if required.
  - Researchers are instructed about the confidentiality rules, and they must comply to and sign documents describing the rules to hold and use SLS data.
  - NRS does not permit direct access to the SLS database to anyone except for nominated NRS staff.
  - Researchers must work under the supervision of their assigned NRS Support Officers at all times.
  - SLS researchers agree the timing of their visit in advance and are accompanied at all time by NRS staff.
  - No computer hardware or additional software installation is allowed into the SLS safe haven.

Only results and final statistical outputs that have been cleared for release by the NRS may be released to the researcher.

All final outputs, including publication must be cleared by the SLS Support Team and checked for disclosure before entering the public domain.

5. Security

Data held by the NRS is protected by tight control and security measures. In NRS, all staff employed:

- Undergo strict security pre-employment checks (Baseline Personnel Security Standard outlined in the Her Majesty's Government (HMG) Security Policy Framework).
- Are continuously trained and reminded about security, data handling and disclosure issues.
- Are bound to multiple data protection legislation such as:
  - the Civil Service Code;
  - census legislation;
  - the Computer Misuse Act, the Freedom of Information (Scotland) Act and the Copyright, Design and Patents Act. Staff using information processing facilities are subject to the IT Code of Conduct.
- Must comply with NRS Information Security, which is approved by the Registrar General and is reviewed on an annual basis each June.

Access Control Policies (ACPs) control the access to information. They apply to any area or system where sensitive or protectively marked data is stored. ACPs apply to all staff.

Access to IT equipment and systems is strictly controlled and all NRS Buildings are secured in accordance with the guidance in the HMG Security Policy Framework.

NRS removable media are encrypted to the HMG approved standard.

NRS has a strict incident management and vulnerability policy for which any security or data misuse must be documented and communicated to Senior Management.

Policies, Documentation and Structure

Information Security and Information Assurance in NRS are in line with the:

- HMG Security Policy Framework,
- Communications Electronic Security Group Information Assurance (CESG IA) Standards and Good Practice Guides.

These standards are closely aligned to ISO 27001.

The organisational structure to protect data privacy and security in each project is based on the Information Asset Owners. They are senior individuals involved in the running of each project that control and grant access to data only to those that need it. They must report to the Senior Information Risk Owner any security issue or privacy concern, who in turn must report to the Accounting Officer, one of the senior officials in NRS.

In NRS, documents and systems are assessed to decide if they must be labelled as protected information. Protectively marked information are subject to internal policies, which are audited on a regular basis, that takes confidentiality, integrity and availability into account and provide a detailed understanding of the risks associated with each system so that individuals can make informed decisions on whether they are suitable

for storing data. Those policies are audited on a regular basis NRS comply with the Data Protection Act and are registered with the Information Commissioner Office's Data Protection Public Register under registration number Z2886501.

Frequent audits of systems and processes are carried out to ensure compliance with the security policies and procedures.

Finally, to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, NRS have defined business continuity plans, procedures, roles and responsibilities.