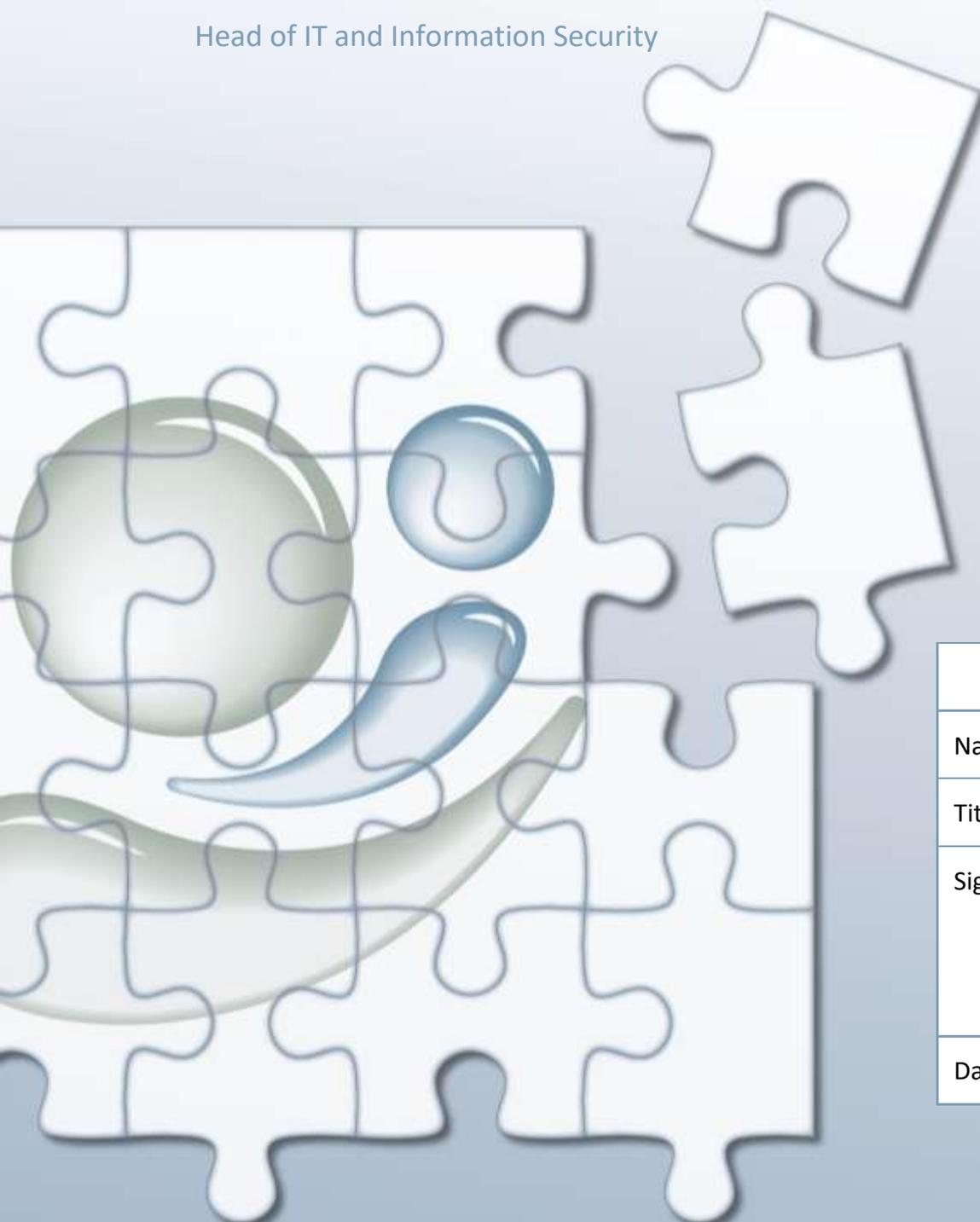


Policy Statement – NPEU

Data Sharing

Author

Head of IT and Information Security



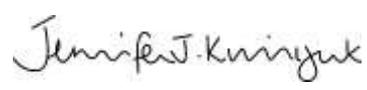
| Authorised by |
|---|
| Name: Jennifer J Kurinczuk |
| Title: Director, NPEU |
| Signature:  |
| Date: 4 th January 2017 |

Table of Contents

| | |
|---|----|
| Table of Contents..... | 2 |
| Document control..... | 3 |
| 1. Introduction..... | 4 |
| 2. Data Sharing with the Research Community..... | 5 |
| 3. Data Sharing with the General Public and Public Organisations..... | 7 |
| 4. Data Sharing with Commercial Organisations..... | 7 |
| 5. Data Curation..... | 8 |
| 6. Data Collection in Future Studies..... | 8 |
| 7. Revision History..... | 9 |
| Appendix 1..... | 10 |
| Appendix 2..... | 11 |
| Annex A..... | 12 |

Document control

Document owner

Head of IT and Information Security.

Document storage

The document is located at F:\ADMIN\Policies

Document approval process

All changes to this document must be approved by the document owner and signed-off by the NPEU Director.

Glossary

- NPEU - National Perinatal Epidemiology Unit
- PI - Principle Investigator
- QA - Quality Assurance
- CAG - Confidentiality Advisory Group
- CI - Chief Investigator
- FOI - Freedom Of Information
- DPA - Data Protection Act
- GDPR - General Data Protection Regulation

1. Introduction

- 1.1. The scope of this policy includes the release of raw data (with personal identifiers or de-identified), aggregate data and analyses which are not released in publications or reports. Excepting that Registers held in the Unit already have long standing data sharing procedures that have been agreed nationally.
- 1.2. The National Perinatal Epidemiology Unit (NPEU) believes that data produced by publicly funded research are a public resource and that as much data as possible should be made available to the scientific community with as few restrictions as possible insofar as this is compatible with the legal requirements for the protection of personal information and within the financial resources available. The types of data held by NPEU and guidelines for their sharing are shown in [Appendix 1](#).
- 1.3. The NPEU has a responsibility to ensure the integrity of any data that it releases for public use and it will not release data to any third party (including collaborators) until all quality issues and queries have been resolved as appropriate.
- 1.4. The NPEU considers that it is entitled (and obliged) to first publication of the data it has generated and to a reasonable but limited period of exclusivity for itself and its external collaborators. This period will be determined for each study and will usually be a minimum of five years following database freeze of a trial or study or five years following the last data collection point for a register or other observational study with on-going data collection.
- 1.5. If a request is made within the 5-year period or prior to the main publication or any planned further publication by the NPEU then the Principal Investigator (PI) can consider a request for data release and pass it for approval to the Unit Director who will have final say on early requests. The decision will take into account:
 - the nature and details of the request,
 - the effect the request will have on any final publication,
 - further analysis or further study,
 - the cost of the early request,
 - the credentials of the requester, and
 - the reasons for the request.

The Unit Director can defer requests until they meet the criteria in 1.3 and 1.4 above.

2. Data Sharing with the Research Community

2.1. Requests for data sharing that meet the criteria in 1.3 and 1.4 above will be considered by the NPEU data sharing committee as appropriate.

- For trials the composition of the Committee will be: Unit Director, Head of Trials, QA Manager, Head of IT and Information Security; with additional members as appropriate, including the current Chief Investigator (CI).
- For archived trials the committee should also include the original CI or members of the original trial steering committee, if available.
- For non-trials, both live and archived, the composition of the committee will be: Unit Director, Senior Statistician, Head of IT and Information Security, the original CI/ principal investigator (PI) if available and others as appropriate.

2.2. The committee will assure themselves that:

- i. the research proposal is scientifically sound,
- ii. the protocol has been peer reviewed,
- iii. there is adequate funding for the proposed work,
- iv. there is appropriate ethics committee approvals in place or in progress.

The committee will require evidence that the likely commitment of NPEU staff has been realistically assessed and will normally expect funding to be available to cover any NPEU costs in making data available and providing on-going support. The committee must also assure itself that releasing the data can be justified within the scope of the original participant consent where applicable or terms of approval where data are collected without consent. Otherwise this approval will have to be sought.

2.3. Data will normally be de-identified before sharing. However, if the nature of the research is such that personal identifiers are required in order to carry it out, NPEU must satisfy itself as to the necessity of providing personal identifiers. NPEU will verify that the requester has adequate procedures and equipment to handle, and protect the data in accordance with principles of data protection as laid down in the Data Protection Act 1998 and the General Data Protection Regulation.

A CAG approval (Section 251 approval from the Confidentiality Advisory Group of the Health Research Authority or any subsequent approval authority) will be required where identifiable data are required:

- When consent has been obtained but the request is for a purpose outside scope of the original consent.
- When Identifiable data have been collected without consent.

2.4. Only de-identified data will be shared with organisations in countries where NPEU deems that data protection law and regulation are less rigorous than the UK or with organisations where NPEU has reason to doubt the rigour of the data protection measures.

2.5. NPEU would prefer to be a collaborator in the exploitation of its data rather than a passive partner and reserves the right to (where it has relevant expertise) propose a partnership to the requesters in the first instance. If the requester declines a partnership or one is not practical, NPEU will reserve the right to peer review any proposed publications or to nominate a suitable peer reviewer. It is a requirement that the authors take into account the scientific comments of the peer reviewers, following which the NPEU may request a re- review.

2.6. Any publications will contain an acknowledgement of the source of the data and of the relevant funding bodies.

2.7. A data sharing agreement will be drafted and agreed between the two parties before any data are released. The agreement will include the following points:

- The requester will undertake not to pass on any data to a third party.
- Named individuals will not be contacted without prior agreement of NPEU, ethics committee and CAG approval (if appropriate).
- Data will only be used for the specified purpose.
- Data are not to be taken home or accessed from remote computers.
- The security measures implemented are at least equivalent to NPEU's own System Level Security Policy. (See [Annex 2](#) for minimum security requirements)
- Disposal and secure deletion of personal identifiers (if released) once they are no longer required.
- Disposal and secure deletion of the entire dataset once the work is completed and publication queries have been dealt with.

- Written confirmation of secure deletion and disposal will be required, including in respect of back-up media.

3. Data Sharing with the General Public and Public Organisations

- 3.1. Members of the public are entitled under the Data Protection Act 1998 and the General Data Protection Regulation 2016, to make data subject access requests to see copies of the information that NPEU holds on them unless an exemption can be claimed that the information will be damaging to their mental health or to their personal safety.
- 3.2. If the NPEU is the Data Controller for data requested under any data subject access request then data will be made available where appropriate and with due consideration of statutory requirements. If a request is received for personal data from an active study NPEU will ask the requester to wait until the study is ended or if they are unwilling to wait, ask that they do nothing to compromise the integrity of the on-going study. If the NPEU is not the Data Controller for data requested under any data subject access request then the NPEU will pass on the request to the appropriate Data Controller.
- 3.3. Freedom of Information Act 2000 (FOI) requests will be passed for consideration by the University of Oxford FOI Office for the appropriate action to be taken. The NPEU will comply with any requests for data from the University of Oxford FOI office.
- 3.4. NPEU will share data with other individuals (e.g. lawyers) or public bodies (e.g. police, local authorities) only if the request is accompanied by signed written consent from the participant or the request is part of an on-going criminal investigation and is accompanied by a court order.

4. Data Sharing with Commercial Organisations

Requests for data sharing from commercial organisations will be considered but unless the informed consent pertaining to the data specifically allows for such an action the participants will be approached (at the expense of the requester and with appropriate ethics

committee and other regulatory approvals) before data release. Payment to NPEU or the participants may be considered as part of the agreement if this is thought to be appropriate by the Data Sharing Committee.

5. Data Curation

- 5.1. NPEU recognises the unique nature of much of the data it has collected and will act as a custodian of the data for future researchers. It will maintain it in a suitable form that minimises deterioration, permits access by bona fide researchers, but protects data from unauthorised users.
- 5.2. When NPEU finds itself in the position of being the sole curator of data from studies where the chief investigator or other senior members of the study team are deceased or otherwise not contactable, it will manage access to the data in the same way as one of its own current studies.
- 5.3. If data from a study carried out at another institution are archived, or the study/trial is archived on behalf of a closed institution, the electronic archive will be held in a separate directory in the main archive but will be managed in the same way as archived NPEU studies.

6. Data Collection in Future Studies

- 6.1. When designing a study, NPEU will consider the practicality and sensitivity of including consent for data sharing at various possible levels, these levels will include:
 - Data to be used only for the specified study
 - Data made available for other research in the same study area (identified or de-identified)
 - Open access to data (identified or de-identified)

Other categories may be included for specific studies.

7. Revision History

This Policy Statement will be reviewed every two years unless there is a major change in data protection law which necessitates a more rapid review.

Appendix 1

Data Categories Held by NPEU and General Guidelines for Sharing

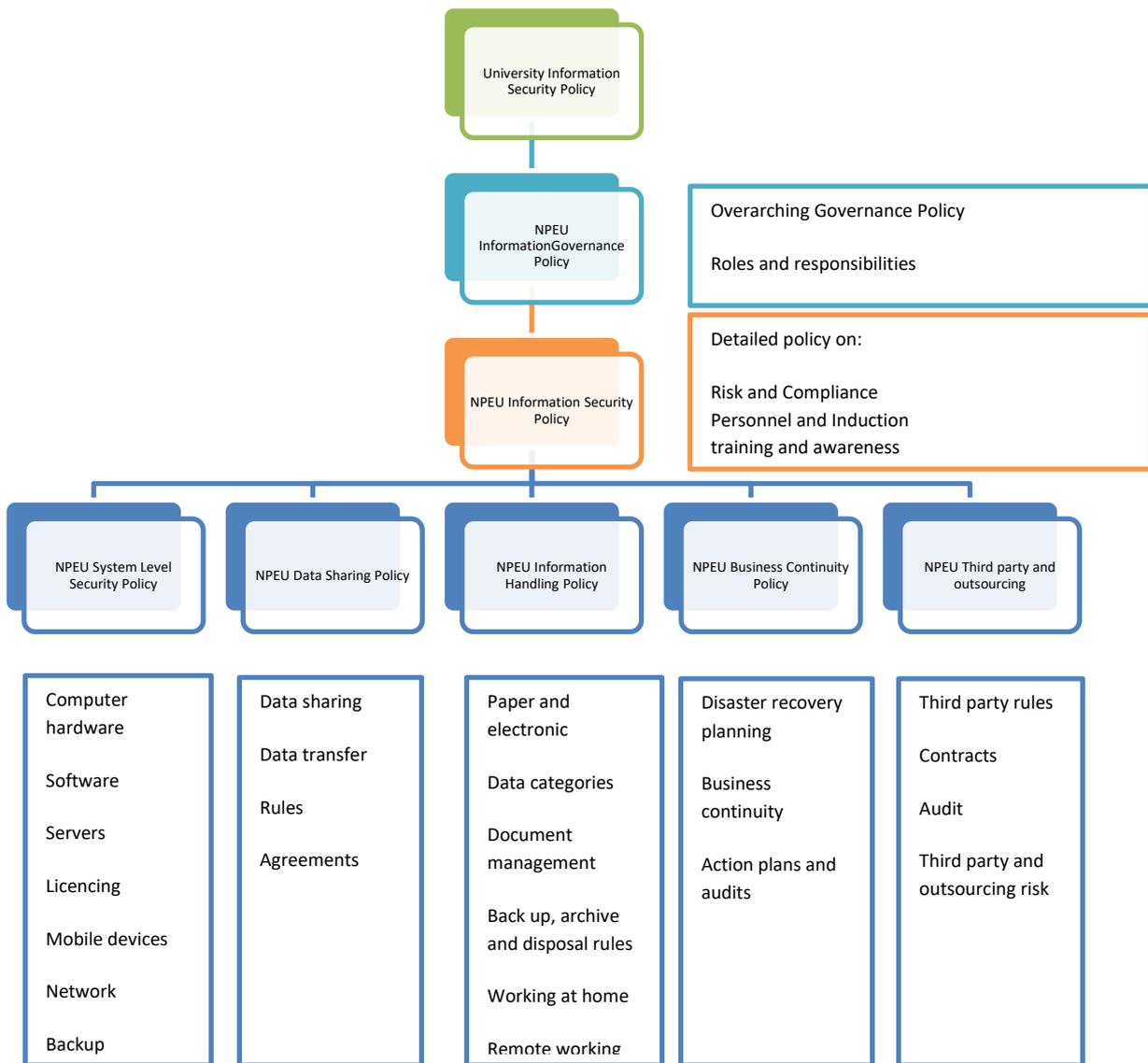
| Type | Consent Held | Share full data including personal identifiers (if held) | Share anonymised data |
|--|--------------|--|--|
| Register study or survey | No | <p>Yes provided that:</p> <ul style="list-style-type: none"> a. Both parties agree that the identifiers are necessary to the research and there are appropriate CAG and Ethics Approvals <p>AND</p> <ul style="list-style-type: none"> b. Both parties are agreed that the work can be carried out without consent (and appropriate approvals are obtained) <p>OR</p> <ul style="list-style-type: none"> c. that obtaining consent is practical and appropriate and appropriate ethics committee and CAG approval is obtained. | <p>Yes Provided that:</p> <ul style="list-style-type: none"> a. Both parties are agreed that the work can be carried out without consent, or that obtaining consent is not practical and appropriate and appropriate ethics committee approval is obtained. |
| Register, Study , Survey or Trial | Yes | <p>Yes, provided that:</p> <ul style="list-style-type: none"> a. Both parties agree that identifiers are necessary to the research and appropriate approvals are obtained <p>AND</p> <ul style="list-style-type: none"> b. The terms of the consent cover the proposed research <p>OR</p> <ul style="list-style-type: none"> c. re-consent is considered practical and appropriate. Then ethics committee and CAG approval will be obtained | <p>Yes, provided that:</p> <ul style="list-style-type: none"> a. The terms of the consent cover the proposed research, and appropriate ethics committee approval is obtained |

Appendix 2

Minimum Information Security Requirements

- Data must be stored in a secure environment and access to the data be restricted and controlled.
 - Ideally data should be stored on file servers in a controlled environment, where access is only given to authorised and authenticated known individuals.
 - Permissions to view and handle data must be restricted to authorised personnel only.
 - Access to data must have a known audit trail.
 - The physical server storage should be in a locked and access controlled rooms.
- Sensitive data or data which contain personal identifiers must never be stored on unencrypted local devices.
- Data encryption must be to a minimum of AES 256-bit encryption.
- Authentication to systems must be by secure password of a strong standard – minimum of 8 characters, at least 3 types of character and changed at regular intervals.
- Data must not be emailed or transferred unless with prior authority of the NPEU Head of IT and Security, and the method of transfer has been risk assessed and approved as appropriate. Sensitive data or data containing personal identifiers must be encrypted prior to transfer and during transfer.

Annex A



- Associated and Supporting Information:**
- Data Protection Act 1998
 - General Data Protection Regulation (GDPR) 2016 (*enters into application 25 May 2018*)
 - The Computer Misuse Act 1990
 - The Regulation of Investigatory Powers Act 2000
 - Freedom of Information Act 2000
 - NPEU Risk Assessment and Information Risk register