Privacy Impact Assessment (PIA): *'Mental Health and Learning Disability Bed Census: One Day Audit'* and the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'*

1. Introduction

The purpose of this document is to report on and assess against any potential privacy impacts as a result of the *'Mental Health and Learning Disability Bed Census: One Day Audit'* and the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'*.

2. Document metadata

2.1 Name of Project

Mental Health and Learning Disability Inpatient Bed Censuses

2.2 Date of report

August 2014

2.3 Authors of report

Health Analytical Services Division, Scottish Government
ScotXed Unit, Scottish Government
Mental Health and Protection of Rights Division, Scottish Government

2.4 Information Asset Owner (IAO) of relevant business unit

Deputy Director, Mental Health and Protection of Rights Division, Scottish Government

Principal Medical Officer, Mental Health and Protection of Rights Division, Scottish Government

2.5 Date for review of Privacy Impact Assessment (PIA)

August 2015

3. Description of the project

3.1 Project background

Scotland's *Mental Health Strategy for 2012-2015* is the successor document to *Delivering for Mental Health* and *Towards a Mentally Flourishing Scotland*[1]. It builds on that work, as well as on policy and service improvements taken forward alongside those main policy documents.

A range of commitments were identified for the period of the strategy. This project acknowledges the wider framework of the Strategy, but will directly focus on Commitment 26:

"We will undertake an audit of who is in hospital on a given day and for what reason to give a better understanding of how the inpatient estate is being used and the degree to which that differs across Scotland.".

Objectives of project

- The objective of this project is to co-ordinate an audit, nationally, of the bed state across Scotland to provide an understanding of who is in hospital on a given day and for what reason.
- The analysis of this information will provide a detailed understanding of how the inpatient estate in Scotland is being used and the degree to which that differs across Scotland.
- In addition to those within Health Board beds, it will be important to identify where patients are 'out of area' in specialist beds, boarding across Scotland and in specialist placements beyond Scotland.

Data will be provided by NHS Boards to the Scottish Government using established statistical data collections methods (further details are provided in this document). Data Sharing Agreements will be put in place between each data provider (NHS Board) and the Scottish Government.

Further information on the content of the statistical data collections can be found in the guidance document and the data specification: http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD.

3.2 Personal data to be processed.

The following personal data will be collected as part of the censuses:

- Community Health Index Number (CHI Number) ^
- Patient Health Record Identifier
- Patient Forename ^
- Patient Middle Name ^
- Patient Surname ^
- Date of Birth
- Gender
- Postcode (of patient's home address)

The project requires patient identifiable variables to be collected at a local level. These will be used to verify the data. Before the data comes to the Scottish Government, data marked with a ^ (patient names and CHI number) will have additional encryption applied to create a 'fingerprint' (i.e. the name/CHI will be converted into a string of numbers). Scottish Government will not be able to decrypt this data, however, the encryption methodology will be shared with National Services Scotland and NHS Central Register to enable future data linkage[1] e.g. for quality assuring the SMR04 data, academic research.

NHS Boards will provide a unique identifier for each patient in the datasets - *'Patient Health Record Identifier'.* If a NHS Board only uses the CHI number as their patient identifier, then they will be provided support to encrypt the CHI number and produce a look up file for local purposes. Scottish Government will only receive encrypted CHI.

The other personal identifiers are gathered for analytical and/or quality assurance purposes.

[1] See section 3.5 for further information

Health Analytical Services Division (Scottish Government) statisticians will receive the following personal data from the ScotXed Unit (Scottish Government) on the dataset which is used for statistical analysis:

- Unique person number (based on encrypted Patient Health Record Identifier)
- Adjusted date of birth – 15/MM/YYYY
- Gender
- Postcode sector (e.g. EH1 3)
- Datazone

Other sensitive data to be processed

In addition, the censuses contain sensitive health information, the full data specification is available at:
http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD

3.3 Processing of data:

The Scotxed Unit (Scottish Government) has extensive experience of gathering sensitive individual level data (for example, child protection data) from a variety of organisations for statistical purposes. Since 2010, Health Analytical Services Division and the ScotXed Unit have received individual level social care data (which includes some health information) from Local Authorities. Health Analytical Services Division and ScotXed Unit will implement the same approach to collect the *Mental Health and Learning Disability Bed Census: One Day Audit'* and the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'* from NHS Boards.

On a single day, each mental health service in Scotland will identify who their inpatients are using current patient management systems in each board. A pre-determined set of data will be collected locally (see the guidance notes[2] for further information). The data will then be uploaded to ProcXed.Net.

ProcXed.NET is a data collection and validation application. It is designed to hold data only for as long as is required to carry out this function. Once the collection and validation process is complete, data is removed.

Access to data in ProcXed.NET is controlled by System Roles. The application is designed to allow for the submitter to retain control of their data whilst they carry out validation on ProcXed.NET. When validation is complete, selecting the Submit option explicitly submits that data to the Scottish Government. Data managers are Scottish Government staff responsible for administering the collection process. Data Managers will, by default, only be able to access the data once it has been explicitly submitted. Access to the data before submission is only permitted on request, where the privacy and sensitivity of the data allows it.

Once data is uploaded to ProcXed.NET it is stored in a physically secure location. In addition, data held on the ProcXed.NET servers is encrypted using AES (American Encryption Standard) encryption (SQL server 2012, operated in fips 140-2 compliant

[2] http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD

mode recommended by the Information Commission's Office). At this point, the Scottish Government become the data controllers.

ProcXed.NET servers are hosted at Pulsant. Pulsant provide physical server hosting including physical security, power and climate control. Pulsant staff have only limited[3] physical access to the ProcXed.NET servers and have no access to the systems.

Pulsant is a secure hosting facility in Edinburgh which is certified to ISO 27001 using a UKAS approved certification body. They provide hosting services to organisations in both the private and public sector. This includes public services such as the NHS and Emergency Services. Many public sector clients hosted by Pulsant have security as a focus and are mandated by the UK government through a Code of Connections (CoCo) (e.g. GSi, GSx, N3 etc) to ensure appropriate security controls are in place. Pulsant has been audited successfully many times by their clients, ISO 27001 auditors, PCI auditors, CESG CLAS consultants and other authorities who advise the UK government on security matters. As part of Pulsant's compliance requirements to ISO 27001, they have implemented an internal audit programme which ensures internal audits are carried out on an on-going basis and findings are reported to management. Their staff are vetted using processes based on the HMG Baseline Personnel Security standard which also requires Disclosure Scotland checks.

Data storage

Data will be stored within the Scottish Government in a data warehouse application called *dbXed* based on SQL Server 2008. For analysis undertaken through SAS® (Statistical Analysis Software), secure connections connect SAS to dbxed, the data warehouse.

dbXed is hosted in the Scottish Government datacentre. The facility is contained with the Scottish Government Saughton House site which benefits from multi camera surveillance and monitoring 24 hours a day. Video cameras are installed inside the data rooms and all doors have access controls. The data centre is designed with the

[3] Only key staff have access under certain circumstances and all access is recorded.

objective of being “a lights out” facility with access only required to install or repair IT hardware. Virtually all systems management activity is completed remotely.

Access to the data rooms is strictly controlled and can only be arranged by following the Data Room Access Procedure. A Permit to Work is required before any moves, adds & changes are carried out and requires the approval of the Data Centre Manager and approval of risk assessment and method statement.

The DC plant is monitored continuously by a dedicated Building and Energy Management System (BEMS). The system provides over 160 different alarms and determines which combination of alarms are critical and require an immediate response. All alarms are reported to the DC plant engineer and critical alarms are monitored on a 7 X 24 hour basis by our Maintenance Contractor who provides a 1 hour on site response.

Data Access

Restricted data access is provided to Scottish Government staff based in the ScotXed Unit (IT), Scottish Government’s internal SAS® Support Team (IT), and Health Analytical Services (statisticians). Access to data is audited.

Data Management

The data will be managed by Health Analytical Services Division and the ScotXed Unit (Scottish Government). Health Analytical Services Division lead (Care Team) statistician approves access to the statistical datasets on behalf of the data controllers (Deputy Director and the Senior Medical Officer, Mental Health and Protection of Rights Division).

Legal basis for data sharing

Data Protection Act 1998

Schedule 2.6: *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.*

Schedule 3.10 - Regulation 9 of The Data Protection (Processing of Sensitive Personal Data) Order 2000: *The processing -*

(a) is in the substantial public interest; (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act); (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

Part IV Exemptions: 33 Research, history and statistics.

- *(1)In this section— "research purposes" includes statistical or historical purposes; "the relevant conditions", in relation to any processing of personal data, means the conditions—*

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

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

(2)For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3)Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely.

(4)Personal data which are processed only for research purposes are exempt from section 7 if—

(a)they are processed in compliance with the relevant conditions, and

(b)the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5)For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed—

(a)to any person, for research purposes only,

(b)to the data subject or a person acting on his behalf,
(c)at the request, or with the consent, of the data subject or a person acting on his behalf, or
(d)in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

Retention Schedule

"Personal data processed for any purpose or purposes shall not be kept longer than is necessary" (Fifth principle, Data Protection Act, 1998). Section 33 of the Data Protection Act states *"Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely".*

The retention of the personal data collected as part of the *'Mental Health and Learning Disability Bed Census: One Day Audit'* and the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'* will be reviewed annually.

Data no longer required will be destroyed in line with Scottish Government IT protocols.

Fair Processing / Privacy Notices

In accordance with the Code of Practice for Official Statistics the Scottish Government have a duty to abide by Principle 5 which covers data confidentiality (as well as to the Data Protection Act 1998). In addition to the processes which will be in place surrounding the transmitting, storing and accessing the data (see above) NHS Boards will asked to update their fair processing notices / privacy notices for patients to inform them of how their data will be used by the NHS Board and Scottish Government. Patients (or their carer) "*have a right to expect that they will be told the purposes for which their information will be used, who will use it, with whom it will be shared, how long it will be retained, and how it can be updated. They further have a right to expect that their information will be handled fairly and securely, and that they will be told all this in a clear and straightforward manner, free from excessively legal*

or confusing language" (Thomas & Walport, 2008[4]). Suggested text to be incorporated by NHS Boards into their fair processing / privacy notices can be found in Box 1.

[4] http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf

Box 1: Privacy Notice – suggested text for NHS Boards (see Annex 3 for easier to read version)

Your personal details may be shared with the Scottish Government, National Records of Scotland and NHS Scotland for statistical and research purposes only.

Your personal details are shared with the Scottish Government, National Records of Scotland and NHS Scotland to allow datasets be joined (or linked) together to improve our statistics and research, for example, to monitor the outcome of a particular disease or illness.

- Every effort will be made to ensure that your information is kept safe at all times.
- Only people in the Scottish Government, National Records of Scotland and NHS Scotland who need to see your personal information will be able to access it.
- All pieces of information which could identify you, such as names and full dates of birth, will be removed before the data is used by statisticians/researchers.

Your health information and care package may be shared with the Scottish Government and NHS Scotland for statistical and research purposes only.

- This information will help the Scottish Government and NHS Scotland plan for future health and care services. This will help improve services for you and others.
- Every effort will be made to ensure that your information is kept safe at all times.
- Your health data will be used to produce statistical information. It will not be possible to identify you from this information.
- The data that health organisations and the Scottish Government hold are potentially very useful for research. We are keen to support researchers who want to use our data. However, they must follow current legal, ethical and privacy guidelines before they can do this.

Examples of the kinds of statistical information which the Scottish Government and NHS Scotland produce can be found here:
http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/Publications

If you would like more information, please get in touch with the following people:

NHS Board contact:

Scottish Government contact:
Statistician, Care Team
Health Analytical Services Division
Scottish Government
Basement Rear, St Andrews House
Regent Road,
Edinburgh
EH1 3DG
0131 244 3777

It is proposed that explicit consent to share data will not be asked of the patients. This is due to several reasons. Firstly, if patients chose to not consent to sharing information then it may result in incomplete datasets and bias – which is of particular importance in statistical analysis and subsequently in service planning. Secondly, although personal data is being collected for linking to other datasets, the end result is an anonymised dataset which will only be used for statistical/research purposes by statisticians and researchers. The data will therefore not be used to influence decisions or actions in respect to an individual or be used to cause substantial damage or distress for that individual. Finally, people who receive mental health services are often very vulnerable and the Scottish Government and NHS Scotland would not be in a position to verify that the patient has fully understood the request for consent and the implications.

3.4 Further data sharing

In order to prevent duplication, data may be subsequently shared with other organisations for statistical/research purposes, including:

National Services Scotland in order to facilitate data linkage (see also section 4) to enable further statistical analysis / research, including:

- The quality assurance of related statistical data collections.
- To facilitate further research by providing access to anonymised data for researchers (e.g. academics) via a safe haven. Further information about this facility can be found here: http://www.isdscotland.org/Products-and-Services/eDRIS/.

National Records of Scotland[5] (formally the General Register Office for Scotland) acting through **NHS Central Register** in order to facilitate data linkage (see also section 4) to enable further statistical analysis / research.

Data on forensics patients may be subsequently shared with the **State Hospital** for further analysis by the Forensic Mental Health Services Managed Care Network.

[5] http://www.gro-scotland.gov.uk/

The **NHS Board responsible for treatment or the NHS Board responsible for funding** may receive a copy of the relevant patient's data for statistical/research purposes.

3.5. Data Linkage

In order to enhance the research and statistics in the area of the mental health and learning disability, the *'Mental Health and Learning Disability Bed Census: One Day Audit'* and the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'* datasets may be made available for data linkage. This will be done under the Data Linkage Framework for Scotland[6].

There are six Guiding Principles which should be considered before undertaking a data linkage project. These can be viewed in detail at:
www.scotland.gov.uk/GuidingPrinciplesforDataLinkage.

In summary, the Guiding Principles are:

1. Public Interest
2. Governance and Public Transparency
3. Privacy
4. Access and Personnel
5. Clinical Trials
6. Sanctions

National Services Scotland and NHS Central Register have data linkage services which are modelled on international data linking best practice. A key aspect of both data linkage services are the separation of personal data to the attribute data. For example:

- Personal identifiers and attribute information (the information about the service the person is receiving and their health condition) is never transmitted and stored together.
- Different teams handle the personal data and the attribute data

[6] http://www.scotland.gov.uk/Topics/Statistics/datalinkageframework

Other key features of using National Services Scotland and NHS Central Register data linkage services include:

- The linking of data is for statistical / research analysis only.
- Data will be transmitted and stored in line with NHS Scotland and/or Cabinet Office data security requirements.
- Data sharing agreements will be put in place between the data controller (Scottish Government) and the organisation responsible for delivering the data linkage service.
- The data used for analysis will not contain patient names and CHI numbers (unless the NHS Board who originally provided the patient data has given explicit consent, patients have been informed and legal and ethical requirements are satisfied).
- Data is accessed through a secure safe haven[7] or via NHS National Services Scotland (ISD Scotland). No copies of the datasets are allowed to be made onto removable media.
- Access to data for analysis is only given to approved analysts for example, they have completed data protection training if they are an academic, and/or they are employed by the Scottish Government, local authority or NHS Scotland.
- Academic researchers must apply to the *'Public Benefit and Privacy Panel for Health and Social Care'* (to be confirmed) to gain access to the *'Mental Health and Learning Disability Bed Census: One Day Audit'*, the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'.*
- All analytical outputs are checked to ensure they comply with confidentiality requirements, for example by applying Statistical Disclosure Control[8]:
    - The aim of disclosure control is to ensure that any statistical analyses will not reveal the identity of an individual or any private information relating to them.

[7] http://www.isdscotland.org/Products-and-Services/EDRIS/
[8] http://www.scotland.gov.uk/Topics/Statistics/About/Methodology/Glossary

4. Stakeholder analysis and consultation

4.1 Groups / organisations involved in the project:

- **Scottish Government: Senior Medical Officers, Policy, Statisticians, IT Specialists**

  Roles:

  1. Designed content of data collection
  2. Consulted on content of data collection with NHS Boards
  3. Put in place permissions.
  4. Put in place IT requirements.
  5. Analysis.
  6. Dissemination.
  7. Project review.
  8. User of analysis to inform service delivery.
  9. User of any related research based on the censuses.

- **NHS Boards: clinicians and service managers**

  Roles:

  1. Designed content of data collection
  2. Data provider
  3. User of analysis to inform service delivery
  4. User of any related research based on the censuses

- **NHS Boards: Caldicott Guardians**

Role: Oversee the use of patient's data

A Caldicott Guardian is a senior person within an NHS organisation who is responsible for protecting the confidentiality of patient and service-user information, and for enabling appropriate information sharing. They play a key role in ensuring that the NHS maintains the highest practical standards for handling patient identifiable information, this includes determining whether to allow the use sharing of person identifiable data.

In Scotland Caldicott Guardians are appointed by Health Boards and each NHS organisation is required to have a Caldicott Guardian.

Caldicott guardians must follow the six Caldicott Guardian principles:

1. Justify the purpose(s) for using confidential information
2. Only use confidential information when absolutely necessary
3. Use the minimum amount of confidential information that is required
4. Access to confidential information should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

More information about the role and responsibilities of Caldicott Guardian can be found on the NHS Scotland Caldicott Guardian website: http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx

5. Questions to identify privacy issues

Will the initiative involve multiple organisations, whether they are public service partners, voluntary sector organisations or private sector companies?

- Yes, NHS Boards, National Records of Scotland and Scottish Government. All the organisations involved have procedures for handling sensitive personal data.

Will it be possible to identify an individual?

- Yes, personal data is shared in order to facilitate data linkage, some data quality checks and analysis (e.g. gender, age). There are strict procedures in place for sharing, storage, linking and accessing (sensitive) personal data (see section 3). Access to any personal data is on a strict need-to-know basis.

- Patients will not be able to be identified from the statistical/research outputs.
    - All analytical outputs are checked to ensure they comply with confidentiality requirements, for example by applying Statistical Disclosure Control[9]:

[9] http://www.scotland.gov.uk/Topics/Statistics/About/Methodology/Glossary

- The aim of disclosure control is to ensure that any statistical analyses will not reveal the identity of an individual or any private information relating to them.

Will there be new or additional information technologies that have substantial potential for privacy intrusion?

- No.

What type of unique identifiers will be used in the project?

- The following personal data will be collected as part of the censuses:
  - Community Health Index Number (CHI Number) ^
  - Patient Health Record Identifier
  - Patient Forename ^
  - Patient Middle Name ^
  - Patient Surname ^
  - Date of Birth
  - Gender
  - Postcode (of patient's home address)

- The project requires patient identifiable variables to be collected at a local level. These will be used to verify the data. Before the data comes to the Scottish Government, data marked with a ^ (patient names and CHI number) will have additional encryption applied to create a 'fingerprint' (i.e. the name/CHI will be converted into a string of numbers). Scottish Government will not be able to decrypt this data, however, the encryption methodology will be shared with National Services Scotland and NHS Central Register to enable future data linkage[10] e.g. for quality assuring the SMR04 data, academic research.

- NHS Boards will provide a unique identifier for each patient in the datasets - *'Patient Health Record Identifier'.* If a NHS Board only uses the CHI number as their patient identifier, then they will be provided support to encrypt the CHI

[10] See section 3.5 for further information

number and produce a look up file for local purposes. Scottish Government will only receive encrypted CHI.

- The other personal identifiers are gathered for analytical and/or quality assurance purposes.

- Health Analytical Services Division (Scottish Government) statisticians will receive the following personal data from the ScotXed Unit (Scottish Government) on the dataset which is used for statistical analysis:

    - Unique person number (based on encrypted Patient Health Record Identifier)
    - Adjusted date of birth – 15/MM/YYYY
    - Gender
    - Postcode sector (e.g. EH1 3)
    - Datazone

- If the data from the censuses are used in any statistical/research data linkage projects, then a 'linkage identifier' will be created for each project and will replace the unique person number (as per Health Analytical Service Division's dataset). This prevents researchers being able to cross reference other data they may have access to through other projects/management information.

Will there be new or significant changes to the handling of types of personal data that may be of particular concern to individuals? This could include information about racial and ethnic origin, political opinions, health, sexual life, offences and court proceedings, finances and information that could enable identity theft.

- Yes. This is the first time Health Analytical Services Division and the ScotXed Unit have conducted the censuses. However, Health Analytical Services Division and the ScotXed Unit have extensive experience of collecting sensitive personal data. Examples of statistical data collections which Health Analytical Services Division and the ScotXed Unit have collaborated on include:

  - Mental Health Benchmarking (includes personal details and health information)
  - Social Care Survey (includes personal details, health information and some financial information)

- Examples of other statistical data collections Health Analytical Services Division are responsible for:
  - Scottish Care Home Census (includes personal details and health information about long stay residents)
  - Scottish Health Survey (includes personal details and health information).

- Scottish Government have strict procedures in place for handling sensitive personal data.

- Guidance and training is available for all Scottish Government staff on the handling of sensitive personal data.

- The subsequent sharing of personal identifiers to facilitate data linkage will follow established procedures, see section 3.5.

- Patients will not be able to be identified from the statistical/research outputs.

Will the personal details about each individual in an existing database be subject to new or changed handling?

- NHS Board staff will extract only the necessary information for the censuses. This information will then be uploaded to ProcXed.Net, which is the secure data collection tool used by the Scottish Government. Scottish Government staff will not have access to NHS Board Management Information Systems.

Will there be new or significant changes to the handling of personal data about a large number of individuals?

- Yes, the censuses are a Scotland-wide one day snap shot of mental health and learning disability inpatient bed use. In addition, information will be collect

on mental health and learning disability inpatients which are funded by NHS Scotland, but are treated out with Scotland.

- For service planning purposes, every mental health and learning disability inpatient bed must be included.

Will the project involve the linkage of personal data with data in other collections, or any significant change to existing data links or holdings?

- Yes, the data from the censuses may be used for future statistical/research projects which involve the linking of datasets. Section 3.5 contains further details.

- Researchers must apply to the *'Public Benefit and Privacy Panel for Health and Social Care'* (to be confirmed) to link any datasets to the *'Mental Health and Learning Disability Bed Census: One Day Audit'*, the *'Mental Health and Learning Disability Patients: Out of Scotland and Out of NHS Placements Census'.*

Will there be changes to data quality assurance or processes and standards that may be unclear or unsatisfactory?

- No.

Will there be new or changed data security access or disclosure arrangements that may be unclear or extensive?

- Scottish Government data security procedures will be followed for the data held by the Scottish Government.

- Any subsequent sharing of data with NHS Boards and the National Records of Scotland will be covered by a data sharing agreement.

Will there be new or changed data retention arrangements that may be unclear or extensive?

- Yes. The organisations involved in this project acknowledge that, in terms of section 33 of the Data Protection Act 1998, personal data processed for research purposes may be kept indefinitely despite the Fifth Data Protection Principle of the Data Protection Act 1998. The arrangements for termination of the data have been agreed as part of a data sharing agreement which will be reviewed annually (or sooner if appropriate).

Will there be changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

- No.

Will the data processing be exempt in any way from the Data Protection Act or other legislative privacy protections?

- Yes, the Data Protection Act Section 33 exemption applies and therefore is exempt from Principle 2, Principle 5 (data retention) and Principle 6 (data subject access rights).

Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

- No.

Does the project's justification include significant contributions to public security measures?

- No.

Is there to be public consultation?

- No public consultation is proposed as the censuses are in response to a policy strategy (Mental Health Strategy for Scotland: 2012-2015[11]) which was previously consulted on[12].

[11] http://www.scotland.gov.uk/Publications/2012/08/9714
[12] http://www.scotland.gov.uk/Publications/2011/09/01163037/0

- Information about the project will be published on the Scottish Government website: http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD

- Patients will be informed of the project through fair processing/privacy notices.

Is the justification for the new data handling unclear or unpublished?

- No. Information about the project will be published on the Scottish Government website: http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD

6. Further information

Further information about the project is available from the following website or by emailing SWStat@scotland.gsi.gov.uk.

http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/DataSupplier/MHandLD

Annex 1: Globalscape (Secure File Transfer) (NHS Scotland National Services Scotland's (NSS) preferred method of sharing data with non NHS organisations)

Transfer of demographic data and (separately) the attribute data (e.g. health information) from the Scottish Government to NHS Scotland will be by Globalscape Secure File Transfer. This is certified as part of the eDRIS[13] solution. Temporary account credentials are machine generated by the Globalscape platform for the upload/download of data. Individual secure drop zones set up for the demographic data and a separate secure drop zone for the attribute data.

Globalscape server infrastructure (HTTPS):

- Web based access to the application encrypted using Secure Socket Layer (SSL)
- Encryption standard SSL 2048 key
- Connection via port 443.

Further information is available on request: SWStat@scotland.gsi.gov.uk.

[13] http://www.isdscotland.org/Products-and-Services/eDRIS/How-eDRIS-is-Secure/

Annex 2: Thru Managed File Transfer (Scottish Government and National Records of Scotland's preferred method of sharing data with other organisations)

SECURITY STATEMENT

Data Transmission & Storage

The DSLS (Data Sharing and Linking Service) implementation of Thru Managed File Transfer uses Transport Layer Security (TLS) encryption in combination with a Server Gated Cryptography (SGC), extended validation certificate to provide the highest available levels of security and trust for data transmission between clients and the server. A minimum of 128bit encryption is applied to any data sent between the server and the client.

Once data is submitted it is stored in a physically secure location (see below). In addition, data held on the servers is encrypted using AES (American Encryption Standard) encryption (SQL server 2008, fips 140-2 compliant as recommended by the Information Commission's Office).

Physical Hosting

DSLS Thru servers are hosted at Pulsant. Pulsant provide physical server hosting including physical security, power and climate control. Pulsant staff have only limited physical access to the servers and have no access to the systems.

Pulsant is a secure hosting facility in Edinburgh which is certified to ISO 27001 using a UKAS approved certification body. They provide hosting services to organisations in both the private and public sector. This includes public services such as the NHS and Emergency Services. Many public sector clients hosted by Pulsant have security as a focus and are mandated by the UK government through a Code of Connections (CoCo) (e.g. GSi, GSx, N3 etc) to ensure appropriate security controls are in place. Pulsant has been audited successfully many times by their clients, ISO 27001 auditors, PCI auditors, CESG CLAS consultants and other authorities who advise the UK government on security matters. As part of Pulsant's compliance

requirements to ISO 27001, they have implemented an internal audit programme which ensures internal audits are carried out on an on-going basis and findings are reported to management. Their staff are vetted using processes based on the HMG Baseline Personnel Security standard which also requires Disclosure Scotland checks.

Application Management

The DSLS Thru application is managed by the DSLS file exchange team. This team has administrative access to the systems. Technical support is provided by the ScotXed unit of the Scottish Government which has access to operating systems and hardware. No other staff in the Scottish Government have administrative access to the systems.

Backup and Business Continuity

DSLS Thru servers are protected by a number of built in hardware countermeasures, such as redundant components and RAID storage arrays and are configured in a high availability clustered configuration.

Data held on DSLS Thru Managed File Transfer is not backed up. This ensures that no additional copies of users data are made. It is the responsibility of the submitter to ensure that they can resubmit their data in the event of a system failure.

DSLS is a central government department, GSI accredited network accredited to handle Restricted material. We are an ISO27001 compliant organisation and as such have business continuity plans, including a risk incident register. This covers the items listed as they are relevant to our business.

Link to Thru Managed File Transfer: https://thru.scotxed.net/

Annex 3: Privacy Notice - Easy Read Version

The Scottish Government is collecting information about people who are in hospital because of their mental health condition or learning disability.

- You do not have to do anything. The Scottish Government will ask for information like your personal details and health details from your health board.

- The information they collect will help the Scottish Government and your health board to plan for health services in the future. This will help to make services better for you and others.

- The Scottish Government will try to make sure that the information they get about you is always kept safe.

- Only people in the Scottish Government who need to see your information will be able to look at it.

- The information that is collected will be used to write a report containing lots of numbers. We call these numbers 'statistics'.

- Scottish Government, the National Health Service and researchers might use other information that is about you to help write their reports. The people who link the information up will not know the health information is about you. The researchers will not know the information is about you.

- No one will know the information that is in the report is about you. Personal information like your name, date of birth and postcode will not be put in the report.

- You can look at the statistics reports by going to this website: http://www.scotland.gov.uk/Topics/Statistics/Browse/Health/Publications

If you would like to know more or have any questions, you can contact the following people:

NHS Board contact:

Scottish Government contact:

Statistician
Care Team: Health Analytical Services Division
Scottish Government
Basement Rear
St Andrews House
Regent Road
Edinburgh
EH1 3DG

0131 244 3777

SWStat@scotland.gsi.gov.uk

Privacy notice (easier to read version) based on original privacy notice used for the Social Care Survey which was produced by the Scottish Consortium for Learning Disability. With thanks to Photosymbols for the images used.

scottish consortium for learning disability
Building respect in the Scottish community

PHOTO SYMBOLS 3

Annex 4: Confidentiality – Code of Practice for Official Statistics

The Scottish Government fully comply with the Code of Practice for Official Statistics. The main principals are:

- Meeting user needs
- Impartiality and objectivity
- Integrity
- Sound methods and assured quality
- Confidentiality
- Proportionate burden
- Resources
- Frankness and accessibility

(http://www.statisticsauthority.gov.uk/assessment/code-of-practice/code-of-practice-for-official-statistics.pdf)

An extract of 'Principle 5: Confidentiality' can be found on the following page along with an explicit protocol around using administrative sources for statistical purposes.

Principle 5: Confidentiality

Private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only.

Practices

1. Ensure that official statistics do not reveal the identity of an individual or organisation, or any private information relating to them, taking into account other relevant sources of information.
2. Keep confidential information secure. Only permit its use by trained staff who have signed a declaration covering their obligations under this Code.
3. Inform respondents to statistical surveys and censuses how confidentiality will be protected.
4. Ensure that arrangements for confidentiality protection are sufficient to protect the privacy of individual information, but not so restrictive as to limit unduly the practical utility of official statistics. Publish details of such arrangements.
5. Seek prior authorisation from the National Statistician or Chief Statistician in a Devolved Administration for any exceptions, required by law or thought to be in the public interest, to the principle of confidentiality protection. Publish details of such authorisations.
6. In every case where confidential statistical records are exchanged for statistical purposes with a third party, prepare written confidentiality protection agreements covering the requirements under this Code. Keep an operational record to detail the manner and purpose of the processing.

Protocol 3: The use of administrative sources for statistical purposes

Administrative sources should be fully exploited for statistical purposes, subject to adherence to appropriate safeguards.

Practices

1. Observe all statutory obligations and relevant codes of practice in relation to the protection of confidentiality and the handling of personal data.
2. Only base statistics on administrative data where the definitions and concepts are good approximations to those appropriate for statistical purposes.
3. Maximise opportunities for the use of administrative data, cross-analysis of sources and for the exchange and re-use of data, to avoid duplicating requests for information. Where possible, use common information technology and information management systems that facilitate the flow of information between producers of statistics.
4. Ensure that no action is taken within the producer body, or public statement made, that might undermine confidence in the independence of the statistics when released.
5. Prepare, in consultation with the National Statistician, a Statement of Administrative Sources which identifies the following.
    a. The administrative systems currently used in the production of official statistics.
    b. Procedures to be followed within the organisation to ensure that full account is taken of the implications for official statistics when changes to administrative systems are contemplated.
    c. Information on other administrative sources that are not currently used in the production of official statistics but have potential to be so used.
    d. Arrangements for providing statistical staff, whether inside the producer body or elsewhere, with access to administrative data for statistical purposes.
    e. Arrangements for auditing the quality of administrative data used for statistical purposes.
    f. Arrangements for ensuring the security of statistical processes that draw on administrative data.