Department of Health
An Roinn Sláinte
Männystrie O Poustie
www.health-ni.gov.uk

HSC Health and Social Care

MEMORANDUM OF UNDERSTANDING (MOU) FOR AN HONEST BROKER SERVICE FOR HEALTH & SOCIAL CARE INFORMATION

Agreed and signed off: September 2013

Last updated: January 2021

Review date: May 2021

MEMORANDUM OF UNDERSTANDING (MOU) FOR AN HONEST BROKER SERVICE FOR HEALTH & SOCIAL CARE INFORMATION

1. This Memorandum of Understanding (MOU) is established for the purposes of informing the development of an Honest Broker Service for Health and Social Care (HSC). The Honest Broker Service enables the provision of anonymised, aggregated and in some cases pseudonymised data from the Regional Data Warehouse, (held within Business Services Organisation BSO), to the Department of Health (DoH) and HSC organisations (listed below). It also provides a service to researchers carrying out approved health and social care related research (*see section 14*).

2. The MOU should be reviewed and kept up to date by the Honest Broker Advice Service (HBAS) in conjunction with the Honest Broker Governance Board (HBGB).

3. A definitions document is provided at Appendix 6.

4. **This MOU has been agreed and signed off by:**

- Health and Social Care Board (HSCB)
- Business Services Organisation (BSO)
- Belfast Health and Social Care Trust
- Northern Health and Social Care Trust
- Southern Health and Social Care Trust
- South Eastern Health and Social Care Trust
- Western Health and Social Care Trust
- The Department of Health (DoH)
- Public Health Agency (PHA)
- Northern Ireland Ambulance Service Health and Social Care Trust (NIAS)
- Northern Ireland Blood Transfusion Service (NIBTS)
- NI Guardian Ad Litem Agency (NIGALA)
- NI Medical & Dental Training Agency (NIMDTA)
- Northern Ireland Practice & Education Council for Nursing and Midwifery (NIPEC)
- NI Fire & Rescue Service (NIFRS)
- Health & Social Care Regulation and Quality Improvement Authority (RQIA)
- NI Social Care Council (NISCC)
- Patient and Client Council (PCC)

(*See section 15- MOU Sign Off*).

5. **Assumptions**

The Honest Broker Service will only provide data in anonymised, aggregated and, where necessary, pseudonymised formats, in line with the General Data Protection Regulation (GDPR), Data Protection Act (DPA) 2018, confidentiality requirements and the ICO's Codes of Practice.

Organisations subject to the MOU should ensure that their Privacy Notices or Fair Processing Notices make service users aware of the uses of their data, including secondary uses[1].

The Honest Broker Service has been developed in line with the ICO's Anonymisation: Managing Data Protection Risk Code of Practice[2] and Data Sharing Code of Practice[3].

6. Scope

The MOU covers the provision of an Honest Broker Service to fulfil 2 purposes:

1) The provision of (or access to) anonymised/ pseudonymised data from the Regional Data Warehouse to other organisations within the HSCNI family, including DoH (see Appendix 3)
2) The provision of anonymised data from the Regional Data Warehouse for approved HSC related research, operating under the "Five Safes" Framework (please see section 14 for more detail on this))

This MOU does not cover the sharing of patient identifiable information.[4]

While this is the current scope for the service provided by the Honest Broker, the service will continue to be reviewed to assess its value and to consider further development of the service.

7. Purpose of an Honest Broker Service

Currently the HSC Trusts (Belfast Trust, Northern Trust, Southern Trust, South Eastern Trust and Western Trust) hold information within the Regional Data Warehouse. This information is used by the individual Trusts, but is not shared across Trusts. The Department, the Health and Social Care Board (HSCB) and PHA require access to data for various purposes including planning, commissioning of services, performance management and public health monitoring.

An Honest Broker Service can help to ensure that this data is shared, within the HSCNI family, including DoH, in anonymised or pseudonymised formats, thus strengthening the protection of health and social care data and patient confidentiality, whilst maximising the uses and health service benefits which can be gained from sharing this information safely.

Previously information was not provided from the Regional Data Warehouse to researchers. The Honest Broker Service enables the safe and secure provision of anonymised data to researchers for approved health and social care related research, which is in the overall interest of public health and the development of health and social care related policy.

[1] See the ICO's Privacy Notices Code of Practice
- https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
[2] ICO's Anonymisation: Managing Data Protection Risk Code of Practice-
https://ico.org.uk/media/1061/anonymisation-code.pdf
[3] ICO's Data Sharing Code of Practice (See ICO publishes new Data Sharing Code of Practice | ICO)
[4] The sharing of patient identifiable information must be managed in accordance to the 'Code of Practice on Protecting the Confidentiality of Service User Information', available from the Department's website https://www.health-ni.gov.uk/publications/doh-hsc-protocol-sharing-service-user-information-secondary-purposes

8. Benefits of Providing an Honest Broker Service

The Honest Broker Service provides:

- streamlined, secure processes for data sharing for the HSC and the Department, creating efficiencies and ensuring full benefits of data sharing for the benefit of public health and well being
- Trusts and others who feed into the Regional Data Warehouse with assurances that the data for which they are responsible will only be made available in an anonymised format in a secure environment to accredited[5] researchers for formally approved purposes
- data to researchers, which could contribute to improved health and social care outcomes and practices and associated benefits for health and social care policy development
- better data security and less data travel
- dedicated research co-ordinators, who are located at BSO offices, to assist researchers with projects and provide advice and support
- statistical disclosure control to protect patient confidentiality.

The Honest Broker Service enables the BSO to maximise data security in the Regional Data Warehouse, while removing the need for excessive procedures across the HSC for access to anonymised/pseudonymised data. Agreement for the Honest Broker Service, via this MOU, should reduce the need for the current number of Data Access Agreements across the HSC, where anonymised and pseudonymised information is required. It provides greater protection of service user information, by increasing the use of anonymised and pseudonymised service user information, whilst supporting the needs of secondary users.

9. Role of BSO

As the Regional Data Warehouse resides within BSO, the Honest Broker Service has been established within BSO, with some resource being provided by the Department for the research support role. In providing the Honest Broker service BSO perform the role of 'data processor', acting on behalf of each of the signatory organisations, (data controllers), who feed data into the Regional Data Warehouse. They carry out the service of taking the data and anonymising or pseudonymising it before providing it to researchers, HSC organisations or the Department.

BSO do not make independent decisions about the further processing of personal data outside of the terms of their engagement under this MOU. If any queries or activity arise which are not included in the instructions under which BSO operate within this MOU, BSO must contact the relevant data controller and seek instructions on how to proceed.

In fulfilling the data processor role, BSO agree to comply with the obligations, equivalent to those imposed on all of the data controllers, by the GDPR Article 5(f) principle - Integrity and confidentiality.

Therefore they must ensure that,

"personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

BSO will ensure that when processing personal data on behalf of the signatory organisations, all of the security considerations of the Integrity and confidentiality principle of the GDPR are met.

[5] Researchers will be considered as accredited once they have completed the Officer for National Statistics Safe Researcher Training.

In providing an Honest Broker service, BSO will:

- Implement systems and processes for ensuring that the data outputs are appropriately anonymised.
- Where pseudonymisation techniques are used, BSO as Honest Broker must ensure appropriate disclosure control to protect the identity of individuals and must ensure that any codes or algorithms used to pseudonymise data are appropriately security controlled and accessed only by the authorised staff. Routine and regular audits should be carried out to ensure this is the case.
- Ensure that data is held and used in a secure manner and is only accessible by authorised personnel.
- Ensure that appropriate vetting and training methods are implemented for staff.
- Ensure that all requests for access to health and social care data are documented and monitored appropriately.
- Remind recipients of their obligations under the law before they access the data.
- BSO may on occasion be required to curate data on specific cohorts as a data asset that can be reused, for example in relation to COVID-19.

10. How the Honest Broker Service Works

BSO, which currently hosts the Regional Data Warehouse on behalf of the Trusts (and the Board), provides a service to process requests for health and social care data which are submitted from within the HSC family (which includes all HSC organisations and the Department). Separately from this they also manage a process for dealing with requests for anonymised data from researchers.

In the majority of cases the outputs provided by BSO are anonymised health and social care data from the Regional Data Warehouse and only anonymised data will be provided for research requests.

The Honest Broker Service provides a safe and secure environment in which the service user data can be processed (and in some cases linked to other data), before being provided in an approved format to the requestor.

Until this most recent review in January 2021 access has been provided through supervised visits to the Honest Broker Safe Haven in BSO Headquarters Franklin Street.

The Honest Broker Service can now also arrange access to the anonymised dataset via the UK Secure e-Research Platform (UK SeRP) based at Swansea University in Wales. The anonymised research dataset would be hosted by the Secure Anonymised Information Linkage (SAIL) databank within Swansea University and researchers then access data remotely through the UK SeRP portal. The choice of safe setting will be determined as part of the application process.

Appendix 4 and 5 provides a diagrammatic overview of how the Honest Broker Service works including further detail about the UK SeRP platform.

11. Provision of Pseudonymised data

On occasion the BSO are required to provide the Department and HSC organisations with pseudonymised health and social care data where this is justified, (for example where there is a need to track trends, which would require a unique identifier).

The pseudonymised identifier must be unique to each individual patient/service user. The method of applying the pseudonymised identifier is via re-coding techniques which are applied to the current Health and Care Number (HCN).

The unique identifier must:

- Remain consistent throughout the life care of an individual patient.
- Consistently be applied across all systems to enable patients to be tracked across all elements of their care and throughout the lifetime of their care.
- Be meaningless to any person outside of the approved staff within the Honest Broker Service and the original Data Controller. The Data Controller may need to link the unique identifier to the HCN and associated data in order to deal with validation queries from organisations using the unique identifier, such as the Department and HSCB. This will ensure that identification of patients and service users outside of the Honest Broker Service or beyond the original Data Controller is prevented.

12. Requests for data from within the HSC or by the Department

- The process for 'Internal' requests received from HSC organisations and the Department is mapped at Appendix 3.
- These are submitted and handled through one point of contact within the Honest Broker Service (within BSO).
- Requests are submitted using the HSC/DoH Application for Data form.
- The Honest Broker ensures that all requests are valid requests (i.e. needed for legitimate purposes) and are for anonymised data.
- If a request is made for pseudonymised data the Honest Broker ensures that appropriate justification has been given for the need for a unique identifier; otherwise the data is provided in anonymised format.
- The Honest Broker has the responsibility of gathering the relevant data and anonymising or pseudonymising that data appropriately.
- Checks are made before the data is shared to ensure that it has been appropriately and correctly anonymised or pseudonymised to ensure that no individual may be identified. (An appropriate checking and approvals process has been implemented by BSO).
- The Honest Broker ensures that only authorised and trained staff access the data and that these staff are fully aware and compliant with data protection and confidentiality obligations. Staff are made aware of disciplinary actions which will be taken as a result of a breach of the terms of the Honest Broker Service, data protection, confidentiality and security.

13. HSC & DoH User Responsibilities

As users of the Honest Broker Service, organisations to which this MOU applies will:

- Ensure they request the minimal amount of data required for the purpose.
- Provide adequate justification when pseudonymised data is required.
- Apply appropriate retention and disposal to the information they receive.
- Will not attempt to identify individuals from the data they are provided, either by using the data they already hold within their organisations, or by linking that data to data received as part of separate requests to the Honest Broker Service.

14. Research and Development Uses

One of the objectives of the Honest Broker Service is to facilitate scientifically sound research through the appropriate use of health and social care data. By providing data for these purposes in anonymised format, the rights of individuals will be respected with adequate privacy protection.

Researchers will only have access to anonymised data and be subject to an obligation not to attempt to re-identify individuals; this and other obligations are outlined in a Research Access Agreement and Disclosure Policy Agreement which researchers must sign before gaining access.

The Honest Broker process for handling research requests is mapped at Appendix 4, the Honest Broker Service operates under the "Five Safes" Framework.

1. Safe Projects - Is this use of the data appropriate, lawful, ethical and sensible?

- Completed applications must provide clear evidence of the value of proposed study to health and social care related research and policies.
- Research limited to secondary use of information previously collected in the course of normal care (without an intention to use it for research at the time of collection) is generally excluded from Research Ethics Committee (REC) review, provided that the patients or service users are not identifiable to the research team in carrying out the research[6].
- However ethical considerations are taken into account as part of the HBS application and if the project requires linkage to data not held in the data warehouse then the Office for Research Ethics Committees Northern Ireland (ORECNI) have advised that REC approval should be sought. For these "Distinct Data Linkage" projects the research team need to ensure appropriate data access agreements are in place. Any decisions taken in relation to unsuccessful applications are fully documented.
- The Honest Broker provides an appeals process for unsuccessful applications.
- The Honest Broker Governance Board is responsible for overseeing the Research Approvals process. Details of the composition of the HBGB and its roles and responsibilities are provided in the HBGB Terms of Reference[7].

2. Safe People - Can the user be trusted to use data in an appropriate manner?

- Researchers accessing data must have appropriate accreditation and training to be trusted to use the data appropriately. This is currently provided through the Office for National Statistics Safe Researcher Training, completion of which is mandatory for accessing data through the HBS.
- Before the data is gathered researchers are asked to sign off an Access Agreement which stipulates the terms and conditions of their use of the anonymised data, including sanctions for misuse, to ensure they will use the data only for the purposes intended and outlined in their application. This must be signed by all researchers involved. An Institutional Signatory is also required by a representative for the organisation with ultimate responsibility for research team members.

3. Safe Data – Researchers can only use data that has been de-identifed

[6] For more information see the "Governance Arrangement for Research Ethics Committees"

[7] The Terms of Reference for the Honest Broker Governance Board will be reviewed annually. To find the latest version of the Terms of Reference please visit the following link: http://www.hscbusiness.hscni.net/services/2843.htm

- The data is gathered by the Honest Broker and anonymised before it is provided to the researcher in a project specific dataset. The dataset is checked and approved before the researcher is given access.

4. Safe Settings - Does the access facility limit unauthorised use or mistakes?

- A safe setting/ 'safe haven' will be used for provision of the anonymised data, this will either be through physical attendance at the supervised HBS safe haven in Franklin Street or through the virtual safe haven provided by the UK Secure e-Research Platform (UK SeRP), hosted by Swansea University. When using the virtual safe haven all outputs will still come through the Honest Broker Service in Northern Ireland for clearance.

5. Safe Outputs - All research outputs are checked to ensure they cannot identify data subjects

- Outputs will only be released once cleared by an appointed contact within the Honest Broker Advice Service, statistical disclosure control is applied to ensure all small counts are suppressed.

15. MOU Sign Off

The MOU has been signed off by the Chief Executives, or equivalent, within each organisation and by the Permanent Secretary of the Department of Health.

In signing the MOU, organisations agree to the establishment of an Honest Broker Service under the terms set out in this MOU. Organisations also agree to abide by the expectations set out for them in relation to their use of the Honest Broker Service and how they handle the data they receive.

The MOU and associated arrangements should be reviewed annually by the Honest Broker Advice Service, in consultation with the organisations included in the MOU.

The MOU Sign Off page is provided at Appendix 1.

This document will be reviewed in May 2021.

Appendix 1

MEMORANDUM OF UNDERSTANDING (MOU) FOR AN HONEST BROKER SERVICE FOR HEALTH & SOCIAL CARE INFORMATION

SIGN OFF

I (print Name), Chief Executive/ Chief Officer for (print Name of Organisation) agree to the establishment of an Honest Broker Service under the terms of this MOU. In signing this declaration, as accountable officer for my organisation, I agree that my organisation will abide by the terms of the MOU. I agree that my organisation will handle the data it receives from the Honest Broker Service in line with the requirements set out by the MOU. I will ensure that staff within my organisation who use the Honest Broker Service, or data from the Honest Broker Service, are aware of their responsibilities and that they are provided with relevant training and awareness to enable them to comply with the MOU.

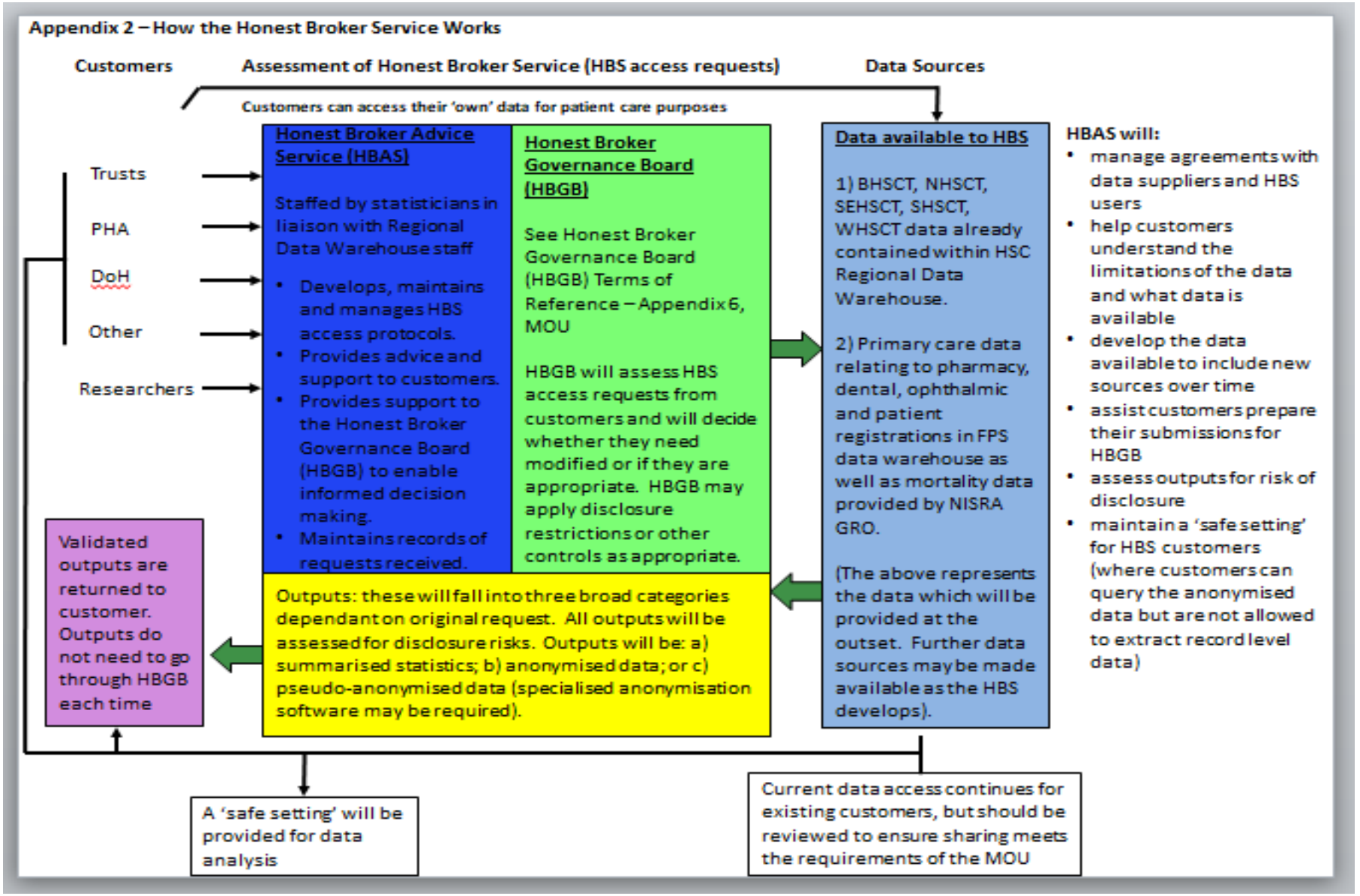
As users of the Honest Broker Service, my organisation and staff will:

- Ensure they request the minimal amount of data required for the purpose.
- Provide adequate justification when pseudonymised data is required.
- Apply appropriate retention and disposal to the information they receive.
- Will not attempt to identify individuals from the data they are provided, either by using the data they already hold, or by linking that data to data received as part of separate requests to the Honest Broker Service.

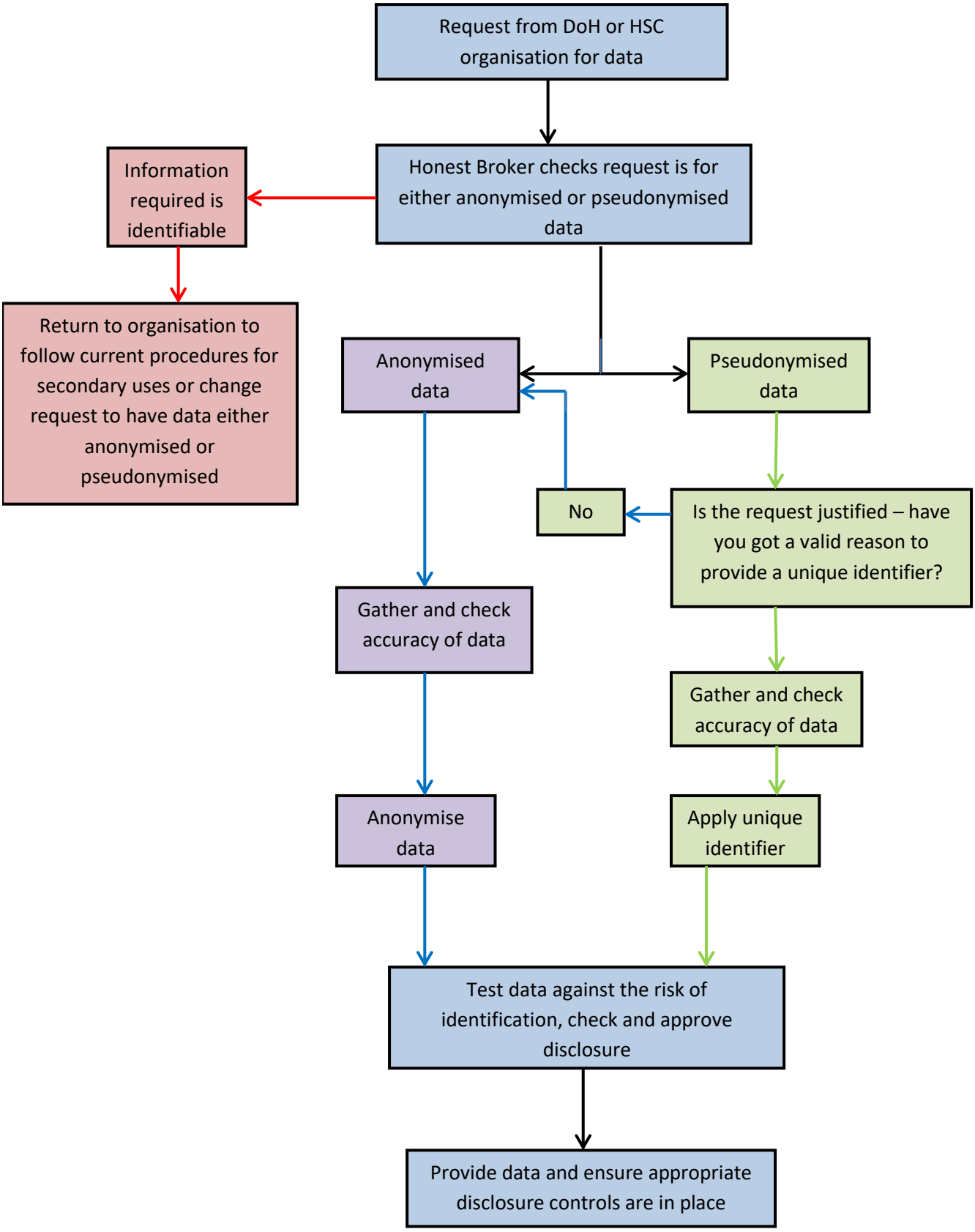
I will ensure that staff are made aware that disciplinary action will be taken as a result of any breach of this MOU and that where breaches occur relevant action is taken.

If I have any concerns over the processing of my organisation's data by BSO, I can request BSO to cease processing the data. I can also request that BSO provide information about their processes for anonymising and pseudonymising the data provided by my organisation.

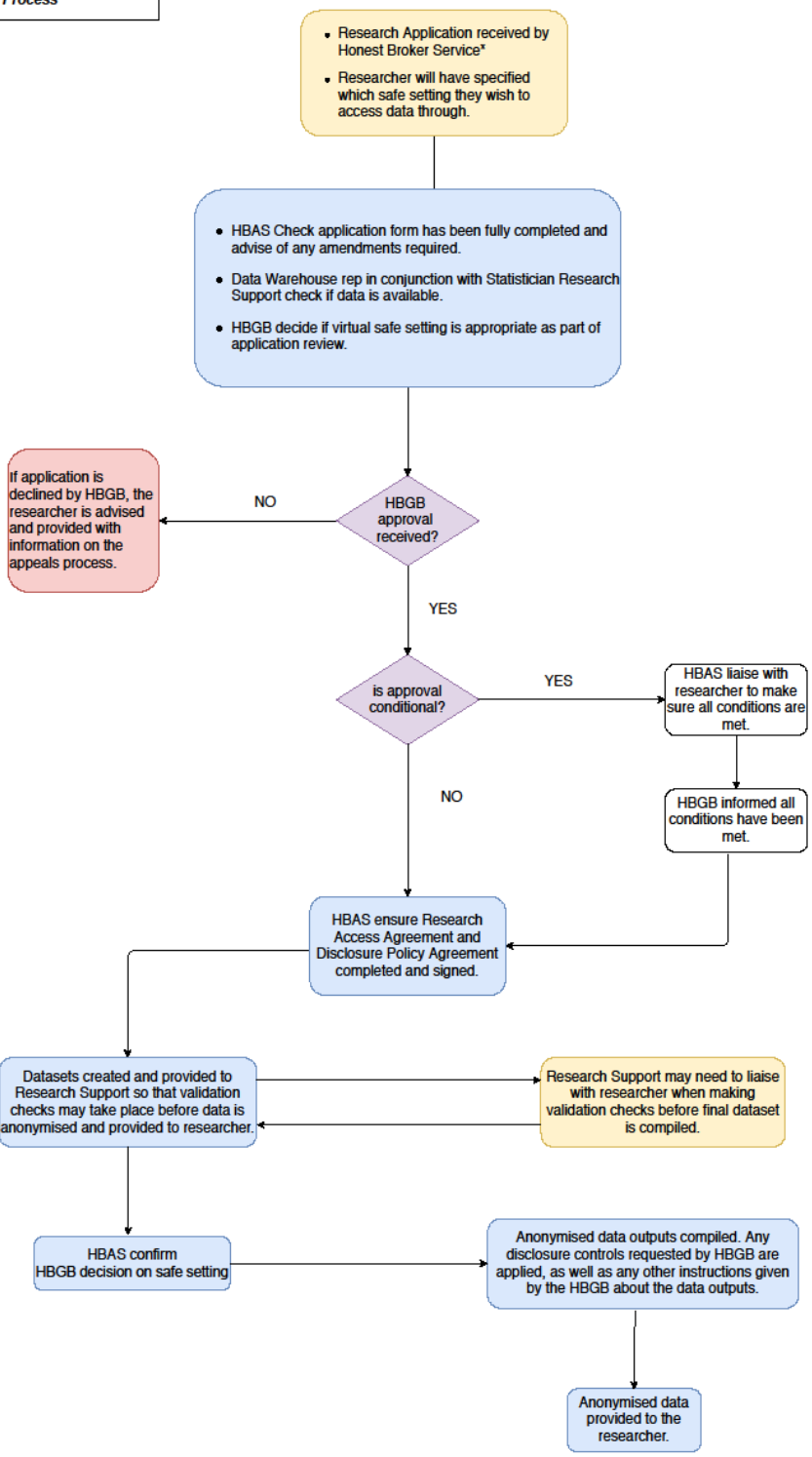
Signature: _____ Date: _____


Appendix 2 – How the Honest Broker Service Works
Customers
Assessment of Honest Broker Service (HBS access requests)
Data Sources
Customers can access their 'own' data for patient care purposes
Trusts
PHA
DoH
Other
Researchers
Honest Broker Advice Service (HBAS)
Staffed by statisticians in liaison with Regional Data Warehouse staff
Develops, maintains and manages HBS access protocols.
Provides advice and support to customers.
Provides support to the Honest Broker Governance Board (HBGB) to enable informed decision making.
Maintains records of requests received.
Honest Broker Governance Board (HBGB)
See Honest Broker Governance Board (HBGB) Terms of Reference – Appendix 6, MOU
HBGB will assess HBS access requests from customers and will decide whether they need modified or if they are appropriate. HBGB may apply disclosure restrictions or other controls as appropriate.
Data available to HBS
1) BHSCT, NHSCT, SEHSCT, SHSCT, WHSCT data already contained within HSC Regional Data Warehouse.
2) Primary care data relating to pharmacy, dental, ophthalmic and patient registrations in FPS data warehouse as well as mortality data provided by NISRA GRO.
(The above represents the data which will be provided at the outset. Further data sources may be made available as the HBS develops).
HBAS will:
manage agreements with data suppliers and HBS users
help customers understand the limitations of the data and what data is available
develop the data available to include new sources over time
assist customers prepare their submissions for HBGB
assess outputs for risk of disclosure
maintain a 'safe setting' for HBS customers (where customers can query the anonymised data but are not allowed to extract record level data)
Outputs: these will fall into three broad categories dependant on original request. All outputs will be assessed for disclosure risks. Outputs will be: a) summarised statistics; b) anonymised data; or c) pseudo-anonymised data (specialised anonymisation software may be required).
Validated outputs are returned to customer. Outputs do not need to go through HBGB each time
A 'safe setting' will be provided for data analysis
Current data access continues for existing customers, but should be reviewed to ensure sharing meets the requirements of the MOU

Appendix 3 – Internal HSC/ DoH Request Process



Appendix 4 – Research Request Process



*If the request is a non research project request from within the HSC family they should follow the internal process for making non-research requests to the HBS (see appendix 3 of the Honest Broker MOU)

Appendix 5 – Business Process Flow for HBS SeRP Use

Standard HBS projects

The majority of HBS projects involve linking HSCNI data from various sources using the Health and Care Number as the main source of linkage.

HBS staff have authorisation to load and remove files from a specific HSCNI area of the UK SeRP server in Swansea. They will be responsible for adding new project folders and managing the researchers user rights to access the data for their specific projects.

This is a similar process to managing the research folders within the current HBS safe haven.

HBS staff are responsible for anonymisation of the research dataset before they are loaded onto the UK SeRP platform.

It is important that this data is fully anonymised; pseudonymised data can be re-identified precisely because it is a reversible process and therefore then counts as personal data under GDPR and DPA 2018.

Any linkage between HCN and study numbers or linkage fields will be broken and the linkage field data will be encrypted prior to loading so that data cannot be re-identified.

This encryption will be project specific to prevent cross identification if users are involved in multiple projects.

In addition to this further measures are in place to prevent re-identification including controls around date of birth (which is always replaced by pre-calculated age, age band or at the very most week of birth), strict controls around geographic identifiers, masking of practitioner codes, aggregation/suppression of certain variables and limiting number of variables provided.

When uploading data to UK SeRP the functionality is place that additional encryption, based on a range of possible encryption methods can be applied to any chosen variable.

The data can only be accessed by the researcher while logged on to the UK SeRP and they are subject to the conditions of their researcher access agreement which precludes attempting to re-identify individuals and outlines penalties for doing so.

In addition to this all outputs are submitted for scrutiny by HBS staff prior to authorising them being released from the system. The HBS staff member assesses the proposed outputs to ensure that any risk of disclosure has been mitigated. Once satisfied, the results can then be released to the researcher.

Distinct Linkage Projects

The LinxMart linkage software has been installed in the HSC Network and all processing of identifiable data takes place within the HSC infrastructure by the Honest Broker Service (HBS). This can be used to match individuals based on demographic data when Health and Care Number is not available.

The process is based splitting each dataset into two components.

Demographic Component – this holds the identifying information to be anonymised.

Content Component – this holds other details, such as diagnosis, medication, etc.

Demographic components are required for data checking and matching, in Northern Ireland the majority of studies are based on matching HSC records using the Health and Care Number as the sole proxy for demographic information.

The Health and Care Number is then used to generate a unique, non-identifiable and encrypted code. This is referred to as an Anonymous Linking Field (ALF).

The ALF is the key to linking different anonymised datasets together so that they can be used in research studies whilst maintaining individual privacy.

Although the ALF is already an encrypted code, SAIL Databank encrypts this again as an additional safeguard. This double encryption means that neither SAIL Databank nor HBS can decrypt the data to patient identifiers.

There are two types of data matching:

Deterministic

Deterministic linkage compares an identifier or a group of identifiers across databases; a link is made if they all agree.

Probabilistic

Probabilistic record linking is based on the assumption that no single match between variables common to the source databases will identify a client with complete reliability. Instead, the probabilistic record-linking method calculates the probability that two records belong to the same client by using multiple pieces of identifying information.

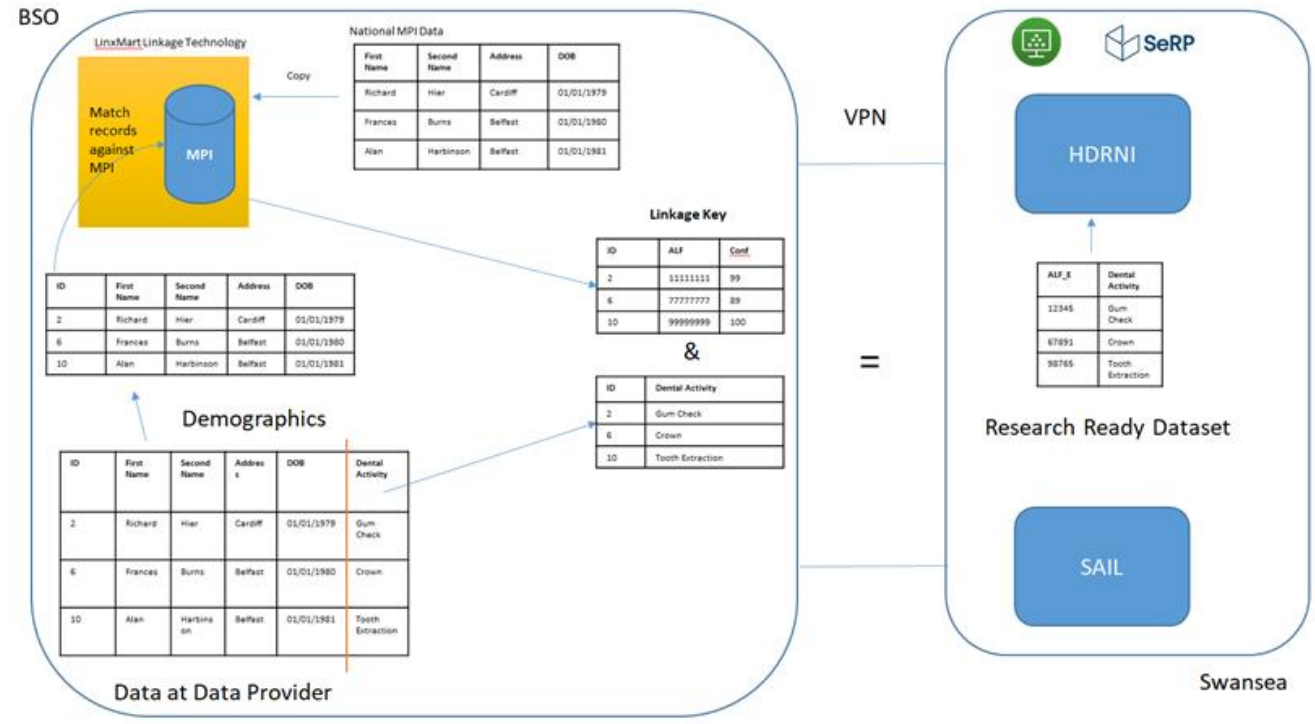
How are the data accessed?

Northern Ireland Research Projects will be subject to the Honest Broker Service approval and governance processes. Approved researchers will be granted access to the SeRP platform through secure login credentials once they have completed all approvals processes, including completion of ONS Safe Researcher training.

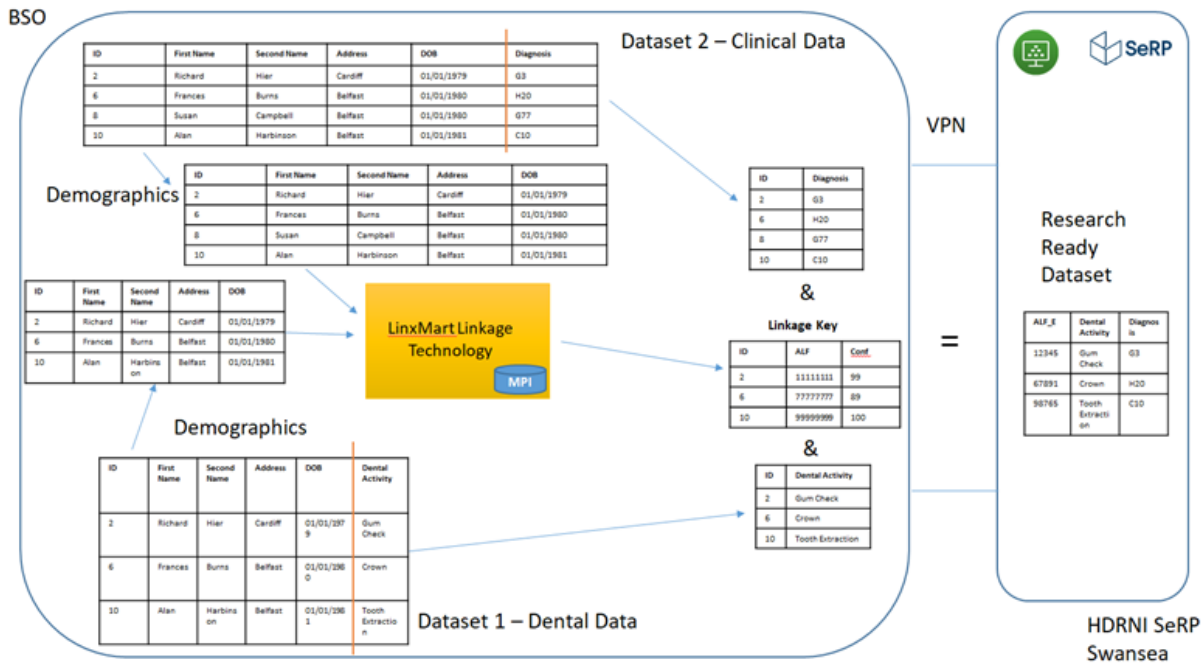
When access has been granted, it is gained through a privacy-protecting safe haven and remote access system referred to as the UK SeRP. This means that research can be carried out in a secure and protected environment.

The standard operating model of SAIL Databank is to provide access to data via the Gateway rather than to release linked datasets. Thus the data are safeguarded from linkage (jigsaw) attacks that may risk individual privacy. These attacks can sometimes occur where someone has a set of anonymised data and uses it in conjunction with other information they hold to attempt to re identify individuals.

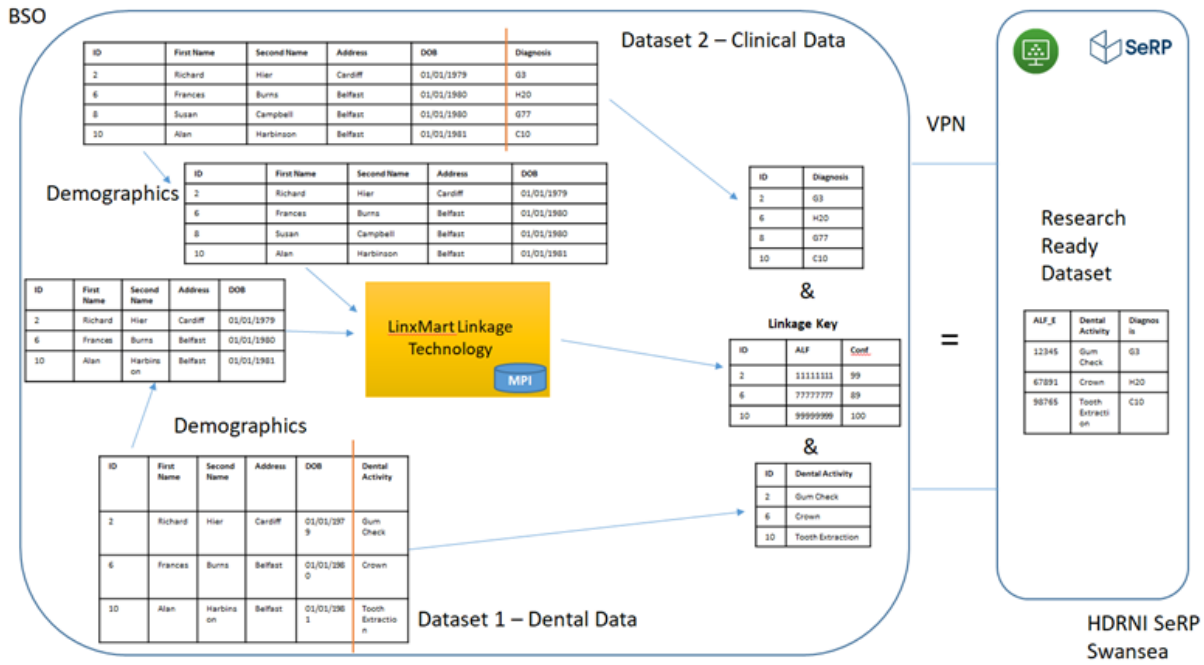
Deterministic Record Linkage Example



Probabilistic Record Linkage Example



Probabilistic Record Linkage Example



Appendix 5 – Definitions

Anonymisation	The process of rendering data into a form which does not identify individuals.
Pseudonymisation	The process of distinguishing Individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Protection Act (DPA)	The main UK legislation which governs the handling and protection of information relating to living people.
General Data Protection Regulation (GDPR)	A regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
Personal Data	Data which relate to a living individual who can be identified- (a) From those data, or (b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Processing of Data	In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including— (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data,

	(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Re-identification	The process of analysing data or combining it with other data with the result that individuals become identifiable.
Safe Setting	Traditionally, a safe setting is a physical location that researchers can enter, with physical controls that ensure they can't take sensitive data with them when they leave. For example, this might be a secure room with a special computer that doesn't have any USB ports, cannot access the Internet. More recently virtual safe settings can be applied such as the UK SeRP which allow data sets can be analyzed remotely from geographically dispersed locations while still retaining security controls to ensure that the data is protected.
Secure Anonymised Information Linkage (SAIL)	The SAIL Databank is a world-class flagship for the robust secure storage and use of anonymised person-based data for research to improve health, well-being and services.
Secure eResearch Platform (SeRP)	SeRPis the complete customisable solution for data sharing, linkage and analysis in a safe, secure and controlled environment that's accredited to the highest international standard.