PSEUDONYMISATION (DE-IDENTIFICATION) POLICY.

Document Reference Information

Version	1.0
Document Status	
Author/Lead	Felicia Ayo-Ajala DPO (Corporate) Ernest Norman-Williams DPO (GPs),
Reviewed by	Abhilash Abraham (Head of IT Security & Cyber security) Kavitha Saravanakumar (Deputy Director of Business Intelligence & Data Management) Simon Carney (Head of Governance)
Directorate	Informatics
Name of Policy	Pseudonymisation Policy
Approved by	Information Governance & Cybersecurity Steering Committee
Date Effective	November 2020
Approved by The Governing	05 February 2021
Date of Next Formal Review	05 February 2022

Version Control Record

Date	Version	Action	Amendments
Nov 2020	1.0		First version
Feb 2021	1.1		Second Version

To be read in conjunction with

- Acceptable User Policy
- Confidentiality Policy
- NHS Confidentiality Code of Practice
- Disciplinary Policy
- Serious Incident Policy
- ISMS Policy

"The CCGs incorporates and supports the Equality Act 2010 and the human rights of the individual as set out in the European Convention on Human Rights and the Human Rights Act 1998"

Table of Contents

1. Introduction

- It is NHS Policy and a legal requirement that, when patient data is used for purposes not involving the direct care of the patient, the patient should not be identified unless other legal means hold, such as the patient consent.

- The NHS Confidentiality Code of Practice states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data.

- Data itself cannot be labeled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

2. Purpose

This policy provides the framework for how NWL Clinical Commissioning Groups (NWL CCGs) will manage the use of patient identifiable data for purposes other than the direct care of patients. Its implementation and adherence will support compliance with legislation and best practice; a number of Data Security and Protection Toolkit ("DSPT") assertions.

A fundamental principle of the Data Protection Legislation - General Data Protection Regulation ("GDPR") and Data Protection Act 2018 ("DPA") - is to use the minimum personal data required for the task in hand. This principle is aligned with the Caldicott Principles. It is supported by the common law confidentiality obligations, the Human Rights Act 1998 and the NHS policy and good practice guidance document, Confidentiality: the NHS Code of Practice, which states the need to 'effectively anonymise' patient data prior to use for non-healthcare medical purposes.

The purpose of this document is to provide guidance to staff so that:

- Personal Identifiable Data ("PID") is processed legally and securely
- It is clear when data should be pseudonymised or anonymised
- Staff know how to pseudonymise or anonymise data
- Business processes continue to be effective in supporting the day-to day operation of the NWL CCGs' business
- Staff knows where to seek advice.

Where the document specifies something '**must**' be done, this is a matter of policy and compliance is mandatory. Where the word 'should' is used, this indicates an expectation of compliance but it is accepted that there may be some element of discretion. All users of such discretion **must** be able to evidence their decision(s) to deviate from the corporate expectation.

3. Scope

- This policy applies to all employees of the NWL CCGs including contracted and temporary staff, volunteers (paid and unpaid), contractors, sub-contractors, members of the Governing Body and its committees, and all those undertaking official CCG business.
- All NHS Commissioners, Commissioning Support Units and providers of NHS commissioned care **must**:

    - ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of patient identifiable data.
    - use the latest DSPT to assist in the implementation and assessment of compliance with policy, procedural and legal requirements.
    - ensure that relevant staff are aware of requirements and are trained to use anonymised or pseudonymised data unless otherwise required by the demands of their role as specified in this policy.

4. Definitions

Pseudonymisation / Pseudonymised Data: Also known as de-identification, is the process involved to enable the NHS organisations to undertake secondary use of patient data in a legal, safe and secure manner.

Pseudonymised (or key-coded) data is where a unique identifier is used to disguise the personal identity but which can be tracked back by the person who has the 'key' Pseudonymisation involves the removing of identifiers from patient data so that a patient/service user may not be identified.

However where multiple sets of data is used, links should be enabled so that it is possible to analyse data sets and trends over time. Individual Service User activity should be able to be identified, but not the Service User themselves.

Anonymised Data: Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. It is important to ensure that anonymisation is conducted effectively and that the data cannot be matched with other data and allow re-identification.

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity.

Anonymisation does not allow information about the same individual to be linked in the same way that Pseudonymisation does and is more likely to be used for 'one-off' queries of data.

Primary Use: Primary use of patient data covers two types, those that directly contribute to the diagnosis, care and treatment of an individual and those used in the audit/assurance of the quality of healthcare provider. This would directly contribute to the treatment, diagnosis or the care of the

individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

Secondary Use Purposes: Where Patient Identifiable Data is used for work not directly related to the care of the patient/service user and when information is processed for non-healthcare and medical purposes. Generally, this could be for research purposes, audits, service management, commissioning, payment by results (PbR), performance management, capacity planning, service redesign and benchmarking, contract monitoring and reporting facilities.

Personal Confidential Data (PCD) essentially refers to any data, or combination of data, that can be used to identify an individual. (PCD), also known as 'Identifiers'

These include, but are not limited to the following:

- Name - including last name and any forename or aliases
- Address – including any current or past address of residence
- Date of birth
- Postcode - including any current or past postcode of residence
- NHS number
- Unique booking reference number Social Service Client number
- Date of death

Confidential patient identifiable data: Any information that can identify an individual. This could be 1 or more of the data items specified in the list above that can be viewed unmodified allowing:

- patients to be identified and differentiated within any subset of
- data patient records to be linked across systems.

Non-confidential patient data: pseudonymised: 1 or more of the data items specified in the list above that can be viewed modified allowing:

- patients to be identified only via secure, Caldicott approved and managed access to related confidential patient
- identifiable data. patients to be differentiated within any
- subset of data.
- patients to be linked across systems.

Non-confidential patient data: part-anonymised: 1 or more of the data items specified in definition of 'PCD' above that can be viewed modified:

- allowing patients to be differentiated within any subset of data but not identified via other data sources and not allowing patients to be linked across systems or subsets of data.

Non-confidential patient data: fully anonymised: None of the data items specified in the definition of 'PCD' can be viewed allowing:
Differentiation by activity codes only – no patient differentiation or identification or linkage across systems or subsets of data.

Aggregate Data: Data derived from records about more than one person and expressed in summary form, such as statistical tables.

Processing data
Processing can mean gathering, using, holding, storing, disclosing, transferring, destroying – anything to do with data management.

5. Roles and Responsibilities

- **Accountable Officer**

  The Accountable Officer has overall responsibility for compliance with the Data Protection Act (DPA) 2018. The Accountable Officer is accountable for information and delegates' responsibility for the development, implementation of, management of information risks, and compliance with this policy, to the Senior Information Risk Owner ("SIRO") and Information Asset Owners ("IAOs") who have specific responsibilities. The Head of IT security, Head of Information Governance and Data Protection Officer is responsible for ensuring that a framework for proper governance and assurance is in place.

- **Caldicott Guardian**

  The Caldicott Guardian will oversee all disclosures or change processes that involve the collection of individual personal information. The Caldicott Guardian **must** review and authorise staff access to Personal Confidential Data (PCD) for Secondary Use Purposes.

- **Senior Information Risk Owner (SIRO)**

  The SIRO is accountable to the Accountable Officer for the management of information risk, with a particular focus on information asset management. The SIRO is the executive lead for pseudonymisation.

- Head of IT Security & Cybersecurity, Director of Business Intelligence & Data Management, Head of Information Governance, DPOs, and HR**'s** responsibilities include:
  - Overseeing the policies and procedures required to ensure compliance with the DPA and subsequent regulations.
  - Overseeing the CCGs' DSPT submissions and ensuring that a 'satisfactory' assessment is achieved.
  - HR to monitor the Data Security and Awareness records to ensure that staff with access to PCD; for Secondary Use purposes have completed the necessary training required.

- **NWL CCG's IG Steering Group**

The NWL IG Steering Group will be the group operationally responsible for the monitoring, compliance and endorsement of all processes related to effective pseudonymisation.

- **Managers**

Managers **must**:

- Identify staff that have a justified purpose to access PCD for Secondary use purposes.
- Ensure that their staff are appropriately trained, utilising the Electronic Staff Record (ESR) Training.
- Regularly review the appropriateness of staff access to PCD
- Organise the removal of staff access rights to PCD, where there is no longer a need for staff to access PCD for Secondary Use purposes.
- Inform the Caldicott Guardian of new staff that requires access to PCD for Secondary Use purposes.

- **Staff**

All staff is responsible for abiding by this policy and guidance and, in discharging their duties in accordance with the law, ensuring that the confidentiality and security of information in all formats is maintained and that any disclosure is appropriate and provided to the correct contact point. In this, they are supported by the procedures, best practice guidance and the NWL CCGs' Information Governance, Data Security and Protection policies and procedures.

Staff with access to PCD for Secondary Use purposes

- **must**: Keep PCD confidential.
- Only use/transfer PCD when authorised to do so.
- Transfer PCD in a secure manner as per agreed Safe Haven
- procedures. When transferring PCD via e-mail to another NHS organisation, NHSmail should be used by both sender and recipients. See the Acceptable Use of E-mail Policy for further details.
- All other transfers of PCD should be via approved secure methods and/or secure networks.
- Anonymise PCD where possible. In any case, the minimum amount of PCD necessary should be used.

Failure to comply with the standards and appropriate governance of information, as detailed in this document, could result in disciplinary action. Staff is also reminded that this document covers several aspects of legal compliance and failure to maintain these standards could result in criminal proceedings against the individual. These include but are not limited to:

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990

.

6 Pseudonymisation/ General Principles

- Personal Confidential Data (PCD) should generally only be used where:
    - There is a direct care-related need to use such data. Patient level data should not contain identifiers when they are used for purposes other than the direct care of patients.
    - Patient consent has been received.

- Where personal data is used for secondary purposes (i.e. non-direct care purposes) such as Research, Audit and Service Evaluation, this data should be pseudonymised. This ensures that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Pseudonymisation supports secondary uses of data whilst maintaining the protection of individuals through preventing their individual personally identifying information being accessed

- Data itself cannot be labeled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

- Safe Haven procedures **must** be used at *all* times when handling and sharing PCD, regardless of whether the data is being used for healthcare purposes or secondary use purposes.

- Staff with access to PCD for Secondary Use purposes **must** be identified.

- Access to PCD for Secondary Use purposes **must** be authorised appropriately by the CCGs' Caldicott Guardian.

- Access to PCD **must** be restricted to authorised users only.

- A register of staff with access to PCD for Secondary Use purposes **must** be created and maintained.

- Staff access to PCD for Secondary Use purposes **must** be periodically reviewed, to ensure that the level of access to PCD is still relevant and appropriate.

- It should also be noted that even where it is legally permissible to use person identifiable information, its use **must** be minimised, for example by only sending a relevant subset of the information, or by the use of one

or more of the techniques described in guidance. This is in line with the Caldicott

principles

- Safe Haven procedures **must** be used at all times when handling

and sharing PCD, regardless of whether the data is being used for healthcare purposes or secondary use purposes.

7 Pseudonymisation Guidance

Processing data

Person Identifiable Data ("PID") may only be processed:

- For Primary Uses (i.e. direct healthcare purposes)
- Where the patient's explicit consent to process PID has been gained
- Where the processing of PID is covered by legislation
- In exceptional circumstances, where processing is justified in the public interest
- Where Section 251, approval has been gained, for the processing of PID

Where data is to be used for Secondary Uses (i.e. non-healthcare medical purposes), and there is no legal basis to disclose PID, data **must** be pseudonymised or anonymised. See Appendix 2 for guidance diagram.

Pseudonymised data

Pseudonymised (or key-coded) data is used to mask the identity of patient data when it is shared with persons for secondary uses. A unique identifier is used and only those with the 'key' can track back to the patient's details.

A typical pseudonymisation will replace the NHS number with an alternative unique number.

Pseudonymisation Notes:

The use of NHS Numbers as the unique identifier is not generally acceptable as this is considered 'weak' pseudonymisation in that there is the potential to easily re-identify an individual. Staff should seek advice from the Head of IT Security & Cybersecurity, Director of Business Intelligence, Head if Information Governance & the DPOs before pseudonymising data by means of the NHS number.

- It should be borne in mind that it may be possible to re-identify patients by a rare disease or particular set of circumstances.
- Data which includes the date of birth and the postcode is not acceptable pseudonymisation
- Dates of birth are difficult to pseudonymise because of the very limited range - replace with age, or month and year, or use age bands
- Postcodes can be too specific, replace with postal town, or the first part of the postcode only.

Ethnic data is classified as sensitive data and should only be displayed where it is relevant to the purpose of the data gathering.

Seek advice from the Data Security and Protection Manager regarding:

- Data relating to patients of less than 13 year of age
- Data covered by the Human Embryology Act and STD Directives, as records should be anonymised in such cases
- Using the date of death

Security

- Pseudonymisation is not a method of anonymisation. Pseudonymised data **must** be treated as PID and be secured appropriately.

- Data Sharing Agreement

  A data sharing agreement should be in place when pseudonymised Information is to be transferred to a third party.

Pseudonymisation process: is the process of distinguishing identities. The aim of such a process (vs. anonymisation) is to be able to collect additional data relating to the same individual without having to know identity.

6. Pseudonymisation can be linked to anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals.

- This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index.

- Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

- Key-coded data is an example of pseudonymisation. This applies to all electronic patient identifiable data, from large databases with thousands of records down to documents or files holding a single item of data, except those used for direct care and those information flows covered by Section 251 regulations for Public Health.

- To effectively pseudonymise data the following actions **must** be taken:

  - An algorithm **must** be applied to the agreed field within the patient record, i.e. the NHS Number to generate a pseudonymised identification number, to be used on reports for secondary use purposes.

  - Each field of PCD **must** have a unique pseudonym.

  - Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff **must** be of the same length and

formatted on output to ensure readability

- Pseudonymisation can be achieved by:

    - Removing patient identifiers;
    - The use of the identifier for example: value ranges instead of age; and
    - By using a pseudonym or multiple organisational pseudonyms

  For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.

- Pseudonyms for external use **must** be independently generated to give different pseudonym from the one used internally in order that internal pseudonyms are not compromised.

- The secondary use output **must** only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines.

- Further wider referencing is available via the following two documents;

    - Connecting for Health Pseudonymisation Implementation Project (PIP), Reference Paper 4 on Pseudonymisation Technical White Paper - Design and MS-SQL

    - http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/pipw hitepaper.pdf

8 Pseudonymisation Controls:

In addition to the organisation's Safe Haven procedures and staff training through the Data security and awareness training, the CCGs currently employs the following Pseudonymisation Controls:

- When data warehouse suppliers and systems are refreshed, Pseudonymisation controls and technology should be implemented where possible, including relevant logging and auditing facilities.

Record of Processing Activities (ROPA) / Data Flow mapping

The NWL CCGS' uses data protection impact assessment ("DPIA") and ROPA to monitor the legal use of PID.

Where new or changed processing of PID is proposed, staff **must** undertake a DPIA and document the new or changed data flows.

This Pseudonymisation Procedure **must** be read in conjunction with the

DPIA to ensure the legal processing of PID.

Access to Person Identifiable Data

The NWL CCGs' uses its data flow mapping process to monitor its information assets and access to person identifiable data.

Information Asset Owners **must** be aware of those persons who have access to their information assets, as well as the reasons for their access.

Those assets which require a Smartcard have additional security procedures including Registration Authority requirements and a regular review by Managers of the access controls granted to staff, in order to provide assurance for the legal processing of PID.

9 Risk Assessment:

It is important to undertake a risk assessment when determining the data to be released prior to publishing, disclosing data to specific recipient(s), or responding to a Freedom of Information Act request.

Assessing the likelihood that personal identity could be revealed is an essential step in meeting the requirements of the law.

Risk Assessment Notes:

Staff should consider:

- The information that is already available that might be used in conjunction with the data to be released to reveal identity
- The information that may become available in future that might be used in conjunction with the data to be released to reveal identity
- The evolving use of technology which could be used to re-identify the data
- Whether there may be people who are motivated to try to discover the identity of individuals within the information to be published
- Potential value of the data to be released for those who might use it to reveal identity (if it were possible)

10 Data Service for Commissioners

- The Data Service for Commissioners Regional Office (DSCRO) is a service which processes data to support local commissioning whilst protecting patient confidentiality in line with the Health and Social Care.
- NHS England has commissioned the HSCIC (NHS Digital), to deliver the new Data Service for Commissioners. The service is delivered by staff seconded into the HSCIC (NHS Digital); from Commissioning Support Units (CSUs), who are part of a Data Management Integration Centre (DMIC).

- The DSCRO service which is hosted by Brent CCG will receive and process personal confidential data (PCD) on behalf of the NWL Collaboration of Clinical Commissioning Groups (CCCGs) within North West London. The establishment of the DSCRO at Brent CCG reduces and in certain circumstances removes the need for NWL CCCGs to handle PCD and allow them to deliver focus on their core commissioning functions.
- The DSCRO follows strict processes to protect the confidentiality of data. Controls are in place regarding the release of data from this service. In particular, personal confidential data (PCD) will only be passed on to other health organisations if there is a lawful basis for that to happen.

Data flows out of the DCRO will be one of the following:

- Aggregate data
- Pseudonymised data, supported by an appropriate data sharing and or processing agreement
- Data for direct patient care
- Identifiable data supported by a relevant S251 agreement
- Where patient consent has been obtained

10 Section 251 Approval

- The section 251 application process is very rigorous and is managed by the Confidentiality Advisory Committee (CAG). Applicants **must** demonstrate that the aim of the processing is in the public interest, that anonymised information could not be used to achieve the required results, and that it would be impractical - both in terms of feasibility and appropriateness - to seek specific consent from each individual affected. For research, the approval of a Research Ethics Committee is also needed. The test is one of necessity, not convenience.

- The powers under the section 251 regulations only provide relief from the common law duty of confidence. Any activity taking place with the support of section 251 **must** still comply in full with the Data Protection Act.

- Section 251 (of the National Health Service Act 2006 and its current Regulations – the Health Service (control of Patient Information) Regulations 2002 - may be used by organisations that have obtained approval from the Secretary of State to use specific confidential information for non-direct-care purposes. The Regulations allow the common law duty of confidentiality to be set aside for medical purposes where anonymised data cannot be used and where obtaining the consent of the individuals concerned is impractical.

11 Safe Havens

Safe haven procedures should be in place in any location where large amounts of personal information is being received held or

communicated especially where the personal information is of a sensitive nature. There should be at least one area designated as a Safe Haven at each of the CCG sites.

- **Location / Security Arrangements**
  Safe Haven environments should be a room that is locked or accessible via a coded key pad known only to authorised staff, or The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.
  If sited on the ground floor any windows should have locks on them. The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage. Manual paper records contained person-identifiable information should be stored in locked cabinets. Computers should be not left on view or accessible to unauthorised staff and have a secure screen saver function and be switched off when not in us. Equipment such as Safe Haven fax machines should be turned off during out of office hours period.

Computers:

- Access to any PC must be password protected, this must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver in use.
- Information should be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.

Personal information of a more sensitive nature **must** be sent over NHSmail with appropriate safeguards:

- Clinical information is clearly marked.
- Emails are sent to the right people.
- Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit.
- The receiver is ready to handle the information in the right way.
- There is an audit trail to show who did what and when.
- Information is not saved or copied into any PC or media that is "outside the NHS".

- **Post**

- All sensitive records **must** be stored face down in public areas and not left unsupervised at any time.
- Incoming mail should be opened away from public areas.
- Outgoing mail (both internal and external) should be sealed securely and, if applicable, marked private and confidential.

- **Phone**

  - Do not make telephone calls where you can be overheard (e.g. Reception)
  - When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their requests in writing where applicable. Where requests have to be dealt with more quickly, the following rules **must** be adhered to. You **must**:
    - be sure that the disclosure is legally-justified and the caller has a legal right to access that information.
    - Verify personal details.
    - Obtain and record the enquirer's telephone number.
    - If the caller is part of an organisation/company, obtain the main switchboard number of that organisation (verifying the number independently via Google / ia phonebook / directory enquiries) and ring back.
    - always provide the minimum amount of information that is necessary.
    - If in doubt, tell the caller you will ring back, where necessary consult a senior manager or the CCG's Caldicott Guardian.
    - All press enquiries for example should be directed to the executive lead for communications.

- **Transporting**

  Where it has been identified that information sharing is to take place with other organisations, information sharing agreements should be documented, agreed and signed up to by the Caldicott Guardians of the partner organisations to that agreement

- **E-mail**

  - Internal E-mail

    The transmission of Patient/Staff Identifiable Data or confidential business within the CCCG is permitted where there is a legal basis for sharing. However information should be kept to the absolute minimum, and should be transmitted in a file which can be password protected.

  - E-mail within the NHS

    The transmission of Person Identifiable Data within the NHS **must** be done by using NHSmail. To obtain an NHSmail account, go to www.nhs.net and register. If there is problem registering

e.g. you are not registered with the CCCGs, contact the ICT Service Desk.

- Internet Email
  Under NO circumstances whatsoever should any patient, staff or business or confidential information be transmitted via internet email (e.g. Hotmail, Yahoo or G-Mail). Due to its insecure nature, any information sent over the Internet should be considered to be in the public domain.

  For more detailed guidance on sending sensitive personal information electronically please also read the Acceptable Use of Email Policy.

- **Short Message Service (SMS) and Texting**

  Under NO circumstances whatsoever should any type of person identifiable patient or staff data be transmitted via SMS.

  Confidential business information should not be transmitted via SMS.

- **Bulk Transfer**
  Bulk transfers of confidential or Person Identifiable Data (50+ records) outside of the CCGs must be authorised by the Caldicott Guardian and Head of Information Governance.

- **Transfer Guidance**
  If you require guidance on securing data in transit please contact the ICT Service Desk.

12 Accredited Safe Havens

- Accredited Safe Havens (ASH) are commissioning bodies, or a designated part of an organisation, which is contractually and legally bound to process data in ways that prevent the identity of individuals to whom the data relates from being identified.

- To maintain ASH status ASHs must provide evidence of completion of level 2 of the Information Governance Toolkit or have a suitable robust improvement plan with timely deadlines to bring them up to a level 2.

- An Accredited Safe Haven may process data that is only weakly pseudonymised; this means the data has the potential to identify an individual if handled outside the controls of the ASH environment (e.g. NHS Number).

- Weakly pseudonymised data may contain the NHS number or the postcode, which on its own will not directly identify the individual, but outside of the controls of the ASH would make the data identifiable.

13 Data locations

This policy applies to data stored on hardware and equipment directly managed, owned or hired by the CCCGs including but not limited to:

- Servers on NWL CCCGs premises
- Any servers on non- NWL CCCGs premises
- Desktop computers on NWL CCCGs premises
- Desktop computers held on non- NWL CCCGs premises
- Laptops, notebooks and netbooks
- PDAs, mobile phones
- Memory cards and memory sticks

14 Pseudonymisation Solution/Design Considerations

In addition to the CCCGs Safe Haven procedures and staff training through the ESR, the CCCGs utilises the pseudonymisation solution provided via North East London DSCRO, specifically.

- **Pseudonym Format**
  One of the objectives for the solution design for the DSCRO was to ensure that the format of the pseudonym cannot be easily confused with actual data item that constitute part of the patient label. This is primarily to avoid situations in which an integer pseudonym is confused with real data item like NHS Number or Date of Birth. The DSCRO use a string that is a combination of alphanumerical characters in upper case. An example value e.g. S1LX97RS26, which cannot easily be confused with any of the common data items but is still readable and therefore can be used in manual processes of data integration and analysis without major difficulties. This format is as well consistent with an approach taken by Secondary Uses Service (SUS) in the pseudonymisation implementation for the national datasets.

- **Different pseudonyms for different organisations**
  One of the objectives is to ensure that there is capability to generate different pseudonyms for the same patient labels made available to different organisations. This is to ensure that even if a pseudonym is compromised in one place this won't affect other data receivers and a real value behind the pseudonym cannot be deducted by dataset comparison. The DSCRO keeps a record of all the data receivers and ensure that unique values are created for each of the data receivers so the same patient label will have different values for each of the data receivers and those values are unique and not duplicated to avoid any unnecessary confusion or mistakes during the data analysis.

- **Existing information systems compatibility**
  Another important consideration is compatibility with already existing information systems. Therefore, pseudonyms conform to PCD data items length and where possible and practical data type too. For example NHS Number is 10 characters long therefore a pseudonym is going to be 10 characters long too.

- **Pseudonym security and re-identification**
  One of the key design considerations is security of the pseudonym - to avoid possibility of unintended re-identification of the actual data item from the pseudonym. To avoid a possibility of cryptographic attack on the pseudonym values match in a true random manner. The random matching prevents a scenario where a compromised batch of pseudonyms would compromise the entire system and allow hypothetical attacker to guess all the current and predict all the future values.

Chosen Approach

- **Approach overview**

  The DSCRO has a hybrid approach to pseudonymisation including sensitive data removal, derivation and random sampling.

  Sensitive data removal is applied to all the strong identifiers apart from postcode. Patient names and addresses are removed from the datasets before any other processing starts. After this is completed if applicable derivation rules are used to derive for example Age from date of birth. Finally random sampling is used to create pseudonyms for all weak identifiers present in a dataset.

15 Training

All staff that has access to any Patient identifiable Data are required to complete the Data Security and Awareness training on ESR.

16 Disciplinary Procedures

- Staff are required to report all incidents involving the loss, inappropriate destruction or unauthorised disclosure of information in line with the NWL CCCGs Incident Reporting policies and procedures.

- All suspected breaches of this policy will be investigated and may be subject to formal disciplinary procedures.

- Serious breaches may result in immediate suspension and/or termination of contract, under the NWL CCCGs' Disciplinary Policy and the Serious Incident Policy.

17 Monitoring and Review

This policy will be reviewed once a year by the Head of IT Security and Cybersecurity, Director of Business Intelligence & Data Management, Head of Information Governance, Head of Governance, and the Data Protection Officers (Corporate & GPs).

18 References and sources

ISO/TS 25237:2008 - Health Informatics Pseudonymisation Standards -	Provides details of the minimum standards for the operation of a pseudonymisation service. Available to purchase from the British Standards Institute website.
General Social Care Council: Code of Practice for Social Care Workers & Employers	These codes of practice set out standards of practice and conduct for social care workers and their employers. Registrants with the General Social Care Council are required to comply with the codes as a condition of ongoing registration.
DH: Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.
DH: The Caldicott Guardian Manual 2010	The Manual is guidance that takes account of developments in information management in the NHS and in Councils with Social Services Responsibilities since the publication of the Caldicott report 1997. It sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader information governance.
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.
The Data Protection Act 2018, General Data Protection Regulation (2016)	https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
Access to Health Records Act 1990	http://www.legislation.gov.uk/ukpga/1990/23/introduction
NHS Code of Confidentiality	http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

DH: Informatics Planning 2010/2011 (PDF, 913 KB)	This Informatics Planning guidance is published alongside the NHS Operating Framework for 2010/11, to provide detailed guidance regarding the informatics elements of local operating plans.
Anonymisation Code	Summary of the Anonymisation Code of Practice

Anonymisation Standard	The Anonymisation Standard for Publishing Health and Social Care Data.
Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013 (PDF, 373 KB)	BSI UK document showing the mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013.
Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 (PDF, 497 KB)	BSI UK document designed to help meet the requirements of the new international standard for information security management, ISO/IEC 27001:2013, which is the first revision of ISO/IEC 27001:2005.
UK Anonymisation Network - useful website	The UK Anonymisation Network (UKAN) has been set up as a means of establishing best practice in anonymisation and offers practical advice and information to anyone who handles personal data and needs to share it.

Appendix 1: Equality Impact Assessment Tool for Policies (Equality Analysis)
To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

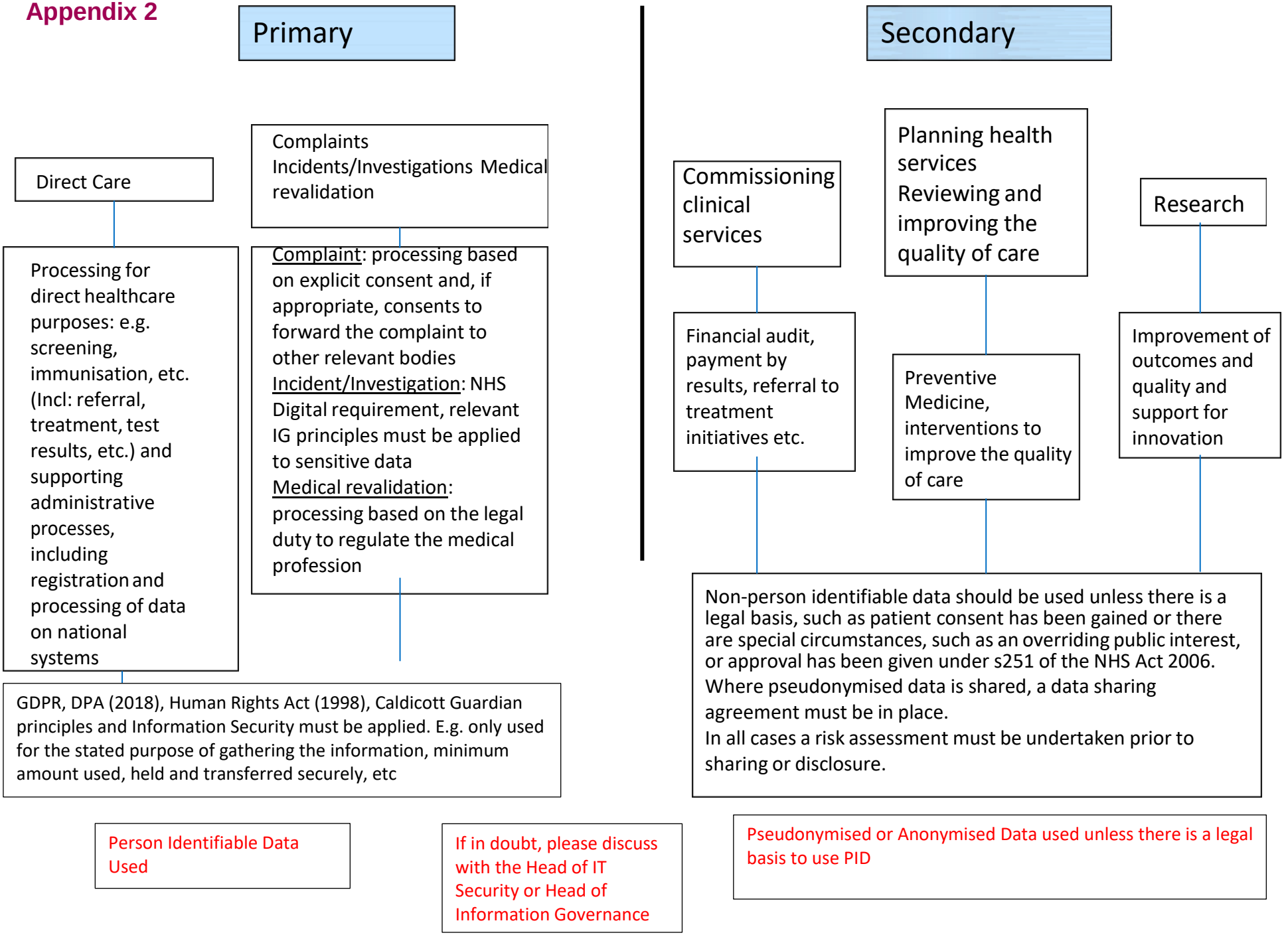
		Yes/ No	Comments
1	**Does the policy/guidance disadvantage one group or more than another on the basis of:**		
	• Race (including colour, culture, ethnicity, nationality or national origin and the travelling community)	N	

	• Religion or Belief	N	
	• Sex (e.g. male or female)	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual)	N	
	• Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.')	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (children, young adolescent, older people etc.)	N	
2	**Is the policy/guidance/strategy more favourably towards one group on the basis of:**		
	• Race	N	
	• Religion or Belief	N	
	• Sex	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation	N	
	• Gender reassignment	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (e.g. children, young adolescent, older people etc.)	N	
3	**If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.**	N/A	
4	**Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?**	N/A	
5	**If so, how would you address the impact? Please explain.**	N/A	

6	**What are the associated objectives to the policy/guidance?**		See section 2 of policy

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.

Appendix 2


Primary
Secondary
Direct Care
Complaints
Incidents/Investigations Medical revalidation
Commissioning clinical services
Planning health services
Reviewing and improving the quality of care
Research
Processing for direct healthcare purposes: e.g. screening, immunisation, etc. (Incl: referral, treatment, test results, etc.) and supporting administrative processes, including registration and processing of data on national systems
Complaint: processing based on explicit consent and, if appropriate, consents to forward the complaint to other relevant bodies
Incident/Investigation: NHS Digital requirement, relevant IG principles must be applied to sensitive data
Medical revalidation: processing based on the legal duty to regulate the medical profession
Financial audit, payment by results, referral to treatment initiatives etc.
Preventive Medicine, interventions to improve the quality of care
Improvement of outcomes and quality and support for innovation
GDPR, DPA (2018), Human Rights Act (1998), Caldicott Guardian principles and Information Security must be applied. E.g. only used for the stated purpose of gathering the information, minimum amount used, held and transferred securely, etc
Non-person identifiable data should be used unless there is a legal basis, such as patient consent has been gained or there are special circumstances, such as an overriding public interest, or approval has been given under s251 of the NHS Act 2006.
Where pseudonymised data is shared, a data sharing agreement must be in place.
In all cases a risk assessment must be undertaken prior to sharing or disclosure.
Person Identifiable Data Used
If in doubt, please discuss with the Head of IT Security or Head of Information Governance
Pseudonymised or Anonymised Data used unless there is a legal basis to use PID