NHS
Kent Community Health
NHS Foundation Trust

Secondary Use of Patient Personal Data Policy

Document Reference No.	KIG021
Status	Final
Version Number	1.4
Replacing/Superseded policy or documents	1.3
Target audience/applicable to	All individuals carrying out work for, and on behalf of, Kent Community Health NHS Foundation Trust, Public.
Author	Assistant Director of Performance and Business Intelligence
Acknowledgements	Not Applicable
Equality Initial Screening Tool / full Equality Analysis (state which)	Equality Initial Screening Tool
Contact Point for Queries	Assistant Director of Performance and Business Intelligence
Date Ratified	May 2022
Date of Implementation/distribution	May 2022
Review date	May 2025
Has this document been adopted?	No
Where has this document been adopted from?	N/A

EXECUTIVE SUMMARY

This policy has been developed to ensure the use of the minimum personal data to satisfy a purpose, and to remove information relating to a data subject that is not necessary for the particular processing being undertaken.

Kent Community Health NHS Foundation Trust (KCHFT) is required to comply with all current data protection legislation in addition to regulatory best practice guidance and national directives when sharing data for purposes other than direct healthcare.

Scope and purpose of Policy

This document seeks to provide all KCHFT Staff who handle patient identifiable data with guidance to safeguard confidentiality when data is used for purposes other than direct patient healthcare, otherwise known as a secondary use. This may include, but not be limited to:

- Healthcare planning
- Commissioning of services
- National Tariff reimbursement
- Development of national policy

This policy will ensure staff are aware of the need to, and how to, ensure patient level information they are sending out has been pseudonymised (stripped of personal identifiable information and replaced with an identifier) or anonymised (all identifiers removed).

IGA produced a document ‘Implementing the ICO Anonymisation Code of Practice providing guidance to Health and Care services on disseminating data into controlled environments. The document outlines the need for consistent use of patient identifiers and the importance of reducing the risk of re-identification to a sufficiently low and acceptable

CONTENTS

Only if required i.e. document is longer than 10 pages

1.0 INTRODUCTION

1.1 When a patient or service user is treated or cared for, information is collected which supports their treatment. This information is also useful to commissioners and providers of NHS-funded care for 'secondary' purposes - purposes other than direct or 'primary' clinical care. Health and social care records about a person are protected not only as personal data under the Data Protection Act 2018 and the General Data Protection Regulation but in most cases also by the common law of confidence and the Human Rights Act 1998.

1.2 There are other statutory restrictions and requirements relating to particular types of health data, including a legal duty to share information, including the NHS Number, in certain circumstances, restrictions on sharing identifiable information about sexually transmitted diseases or fertility treatments and both permissions and restrictions that can be applied under care sector specific regulations.

1.3 By anonymising data, users are able to make use of patient level clinical data for a range of secondary purposes without having to access the identifiable data items.

1.4 Anonymisation is achieved by reducing the risk of re-identification to a sufficiently low and acceptable level. The purpose of this guidance is to explain how to anonymise a health and social care dataset before it is disseminated into a controlled environment, the steps that should be taken to reduce the risk of re-identification associated with a dataset, and the controls needed in an environment to reduce residual risk to an acceptable level.

1.5 In addition to anonymisation, data can also be pseudonymised or be identifiable when shared. If identifiable data is required, there are many controlling factors to be considered such as consent, legal basis or legitimate interests, It is therefore essential to be aware of current legislation and to ensure the rights of all individuals are protected and respected at all times.

1.6 This policy will explain the differences between each of these data types and provide guidance on proceeding in all cases.

1.7 If in any doubt about the data format or concerns over whether the sharing is permissible under law or best practice contact the Performance team on kcht.performanceteam@nhs.net who will be able to advise.

1.8 Alternatively for generic advice in regard to information sharing or guidance in regard to information sharing agreements contact the Information Governance team kcht.informationgovernance@nhs.net .

2.0 ANONYMISATION LEGISLATION AND GUIDANCE

2.1 Health and social care information that identifies an individual will in most cases be confidential, and protected in law by the common law of confidence and by Article 8 of Human Rights Act 1998. It is also personal data, and special categories of personal data, under the Data Protection Act 2018 and the General Data Protection Regulation.

2.2 These laws impose conditions on health and social care information about an individual being disseminated from one person to another, or from one organisation to another; for example, if the information is confidential it may be necessary to first have the person’s consent. Gaining consent or identifying another lawful basis for dissemination may be impracticable, or even impossible.

2.3 Patients can be identified using various personal details, alone or in combination. Patient identifiable information includes the following:

- Forename
- Surname
- Initials
- Address (inc. postcode)
- Telephone Number
- Date of Birth
- Sex
- Postcode
- NHS Number
- Ethnic Group

2.4 A combination of one or more of these can be used to identify a patient. When supplying data for secondary use that includes any of the above then guidance should be sought as to whether the level of detail is sufficient to be identifiable.

Example

In isolation, a postcode may not appear to be patient identifiable. However, in some rural areas a postcode can cover a very small number of properties and therefore be used to identify individual patients. The more of the above information that is shared, the higher the risk of individuals being able to be identified.

3.0 PSEUDONYMISED INFORMATION

3.1 Pseudonymised information is where the most identifying fields within a set of data have been replaced with artificial identifiers, or pseudonyms. For example, a name or in most cases, NHS Number, is replaced with a unique number. The purpose is to render the data record less identifiable and therefore reduce concerns with data sharing and data retention.

3.2 Pseudonymisation should be used where data is for secondary use and needs to be shared with the intention of linking data sets and over time using a common pseudonym. If this process is required then please contact the Performance Team (kcht.performanceteam@nhs.net) who have access to Pseudonymisation tools.

3.3 Pseudonymisation allows the linking of data where an identical Pseudonymisation process has been applied, and is therefore reversible using the same process.

4.0 ANONYMISED INFORMATION

4.1 Anonymised information is different to pseudonymised information in that anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. Therefore, once the anonymisation process has taken place the data has permanently become non-identifiable and cannot be reversed.

4.2 Where health and social care information about a person, or about a group of people, is effectively anonymised, no further action is required to satisfy either the Data Protection Act 2018, the General Data Protection Regulation or the common law of confidence – the data are no longer subject to either. As long as individuals are very unlikely to be identified by the recipient(s), the anonymised data may be published or disseminated to specific organisations or people.

4.3 Anonymisation enables health and social care data to be shared more widely than would otherwise be possible for purposes such as research, clinical audit, and health care commissioning to bring public benefit. This is one important reason for anonymising health and social care data. Another is that data protection law requires the minimum necessary personal data to be used to satisfy any particular purpose – where anonymised data would suffice; it should be used in preference to identifying data.

5.0 NATIONAL DATA OPT-OUT

5.1 Individuals have the right to opt out of their information being used for secondary purposes. NHS Digital has developed a system to support the national data opt-out which gives patients more control over how their personally identifiable data is used.

5.2 Patients who decide they do not want to share their personally identifiable data for planning and research purposes are able to set their national data opt-out preference online at nhs.uk/your-nhs-data-matters. NHS Digital provides a non-digital alternative for patients who can't or don't want to use an online system. The preference will be set once and apply to all data sharing for planning and research purposes.

5.3 All staff need to be aware of the national data opt-out so that they can advise patients about the benefits of sharing data, the choices they can make and where they can find more information. This is so patients can make an informed decision about how their personally identifiable data will be used. Further guidance can be found at https://digital.nhs.uk/national-data-opt-out

5.4 Data that has been anonymised will not be subject to the national Opt-Out and can therefore be shared.

5.5 All confidential patient identifiable data that is being shared outside of KCHFT should be assessed against the national data opt-out criteria to establish if records for patients who have registered their opt-out preference need to be removed.

6.0 PSEUDONYMISATION/ANONYMISATION PROCESS

6.1 In the first instance, if a request has been made for patient level data, you should contact the Performance Team on kcht.performanceteam@nhs.net to ascertain if the data request is valid.

6.2 Once the request to share patient level data for secondary use has been accepted, an evaluation needs to take place as to the level of detail provided.

6.2.1 If the data needs to be Pseudonymised, then patient choice needs to be considered in terms of opt-out to ensure data for patients that have opted out is not shared. In this instance, contact the Performance Team to assist with Pseudonymisation.

6.2.3 If the data is not required at patient level, the following anonymisation process needs to be followed, which the Performance Team is available to support in:

6.3 Assess Data Characteristics

6.3.1 Determine how many data subjects or events are included in a data set, whichever is the greater, e.g. a data set may contain data on 1,000 different individuals or on 1,000 events which may relate to the same or different individuals. Risk factors arise from large datasets that may be seen as tempting targets and from small datasets where a data subject loses the ‘safety in a crowd’ protection.

6.3.2 Direct identifiers such as name, address, telephone number, e-mail address, ID numbers where look-up facilities are available to the public, are prohibited.

6.3.3 How current is the data, how long will it be retained and does it enable person level data about the same individual to be tracked over multiple years?

6.3.4 What is the smallest value that might appear in any cell. This may well be unknown prior to the data being produced but setting a minimum value and ensuring that it applies throughout the data can be an effective way of reducing risk.

6.4 Data Minimisation

6.4.1 The aim of data minimisation is to identify the minimum amount of data required to fulfil the purpose of the dissemination, and to exclude any excessive data.

6.4.2 The Data Protection Act requires that: 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'

6.5 Data Manipulation

6.5.1 Once the minimum data requirements have been established and removed all direct identifiers, consideration needs to be given to whether techniques that involve manipulating the data might be applied to reduce the risk factors that will be generated by the data characteristics.

6.6 Establish Risk Factors

6.6.1 Following data minimisation and data manipulation the data characteristics may have changed or risk mitigations put in place so the Risk Factors associated with the remaining data need to be established. Risk Factors are calculated differently for aggregated and individual level data. For individual level data there are five areas to be considered:

- Scale
- Linkage and disclosive characteristics
- Impact and motivation
- Temporal characteristics
- Potential Identifiers

6.7 Adjust for Data Manipulation

6.7.1 Data manipulation techniques such as Pseudonymisation can reduce the risk of data subjects being identified from data and so can provide an adjustment to the risk. Once the basic risk factors have been calculated an adjustment should be made to reflect any data manipulation techniques used and the reduced risk of re-identification that results. Whilst data manipulation techniques apply predominantly to aggregated data, sampling and swapping techniques can be applied to individual level data in circumstances individual outcomes etc for all data subjects do not need to be tracked.

6.8 Determine a Control Plan

6.8.1 Environments must have a minimum level of controls (e.g. stored on encrypted drives, transferred via secure email accounts) to keep data safe and secure for them to be considered sufficiently controlled to handle data in a safe and secure manner. If data is to be disseminated into a controlled environment (Safe Haven) the controls must be sufficient to reduce the risk of data subjects being identified to an acceptably low level. If risk cannot be reduced to an acceptable level the approach must be revisited and the data characteristics (identifiable data fields) changed to reduce risk factors. If you are unsure if the risk has been reduced sufficiently, please seek guidance from the Performance or IG teams.

6.9 Review Outputs to Ensure Non-Identifying

6.9.1 Even where risk is thought to have been reduced to an acceptable level, it is extremely important that final dataset(s) that are due to be shared are checked to ensure no errors, anomalies or vulnerabilities have escaped detection. If necessary, contact the Performance Team who can double check for you.

6.10 Governance/Sign-Off Process

6.10.1 In the absence of previously agreed criteria that have been accepted by an organisation (e.g. as part of a negotiated information sharing agreement) the governance process should involve the Performance Team for final sign-off (who will in turn seek guidance from the IG team or Caldicott Guardian if necessary)

7.0 ROLES AND RESPONSIBILITIES

7.1 Objective

7.1.1 To establish the management structure for good practice to anonymise data effectively and comply with national guidance and legislation within KCHFT.

7.1.2 KCHFT will issue and regularly review the policy to ensure staff are provided with clear guidance on the anonymisation of data.

7.2 Trust Board

7.2.1 The Trust Board has the ultimate responsibility for compliance with data protection legislation and associated best practice including the ICO Anonymisation Code of Practice

7.3 Heads of Service / Managers

7.3.1 Ensure that all staff are aware of their responsibilities with regards sharing of patient identifiable, pseudonymised and anonymised information.

7.4 Staff

7.4.1 Everyone managing and handling patient identifiable information is aware of her/his responsibilities and obligations to follow the Anonymisation Code of Conduct when sharing data.

7.5 Performance Team

7.5.1 The Performance Team have final sign-off of data requests that have been either anonymised or pseudonymised to check for compliance with this policy and national policies and procedures.

GOVERNANCE SCHEDULE

Ratification process

Governance Group responsible for developing document	*Information Governance Assurance Group*
Circulation group	*Intranet, Policy Distribution*
Authorised/Ratified by Governance Group/Board Committee	*Information Governance Assurance Group*
Authorised/Ratified On	*May 2022*
Review Date	*May 2025*
Review criteria	*This document will be reviewed prior to review date if a legislative change or other event dictates.*

KEY REFERENCES

These are key documents that the policy, guideline, SOP etc. relies on for best practice or national guidance or a legislative requirement. It is a list of those items that have been relied on for best practice and influence the requirements of the document.

Title	**Reference**
Information Governance Alliance Implementing the ICO Anonymisation Code of Practice: Guidance for Health and Care Services on disseminating data into controlled environments	N/A
ICO website www.ico.gov.uk for codes of practice	N/A
Data Protection Act 2018	N/A
Common Law Duty of Confidentiality	N/A
Department of Health document 'Your Data: Better Security, Better Choice, Better Care' (July 2017)	N/A
Human Rights Act 1998	N/A
General Data Protection Regulation	N/A
Being Open Policy (incorporating Duty of Candour)	IML004
Confidentiality Code of Conduct	KCRM005
Cyber, Network and Information Systems Policy	KIG026
Data Security and Protection Policy	KIG025
Data Quality Policy	RM008
Freedom of Information Act 2000 Policy	KIG017
Incident Policy	CQS016
Transfer of Care Policy	QC003

DOCUMENT TRACKING SYSTEM

Version	Status	Date	Issued to/Approved by	Comments/Summary of Changes
0.1	Draft	January 2018	Flo	For 2-week consultation period
0.2	Draft	March 2018	IGAG (approval)	Increased size of appendix. Approved
0.2	Final	March 2018	Corporate Assurance and Risk Management Group (ratification)	Submitted for Ratification Ratified at CARM 18th April 2018
1.0	Final	June 2018	IG Assurance Lead	Version number updated and published on Flo.
1.1	Draft	January 2019	IGAG (virtual approval)	Audit process included
1.2	Final	January 2019	AD of Performance and Business Intelligence	Reference to KIG011 removed
1.3	Draft	July 2019	IG Assurance Lead	Section 5 renamed and wording updated slightly
1.4	Draft	May 2022	AD of Performance and Business Intelligence	Reviewed and updated to new policy template
1.4	Final	May 2022	IGAG (virtual approval)	Approved

Summary of Changes

a. *Moved to new Policy template*

Has an Equality Analysis (EA) been completed?

No ☐

The document will have no impact on people with any of the nine protected characteristics

Yes X

Include summary of any reasonable adjustments or actions required to avoid significant impact on patients, patients' families and employees and volunteers with protected characteristics.

The Equality Analysis for this policy is available upon request by contacting the Engagement Team via kchft.equality@nhs.net.

NOTE:

Kent Community Health NHS Foundation Trust is committed to promoting and championing a culture of diversity, fairness and equality for all our staff, patients, service users and their families, as well as members of the public.

Understanding of how policy decisions, behaviour and services can impact on people with 'protected characteristics' under the Equality Act 2010 is key to ensuring quality and productive environments for patient care and also our workforce.

Protected characteristics: *Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex, Sexual Orientation.*

An equality analysis should be completed whilst a policy is being drafted and/or reviewed in order to assess the impact on people with protected characteristics. This includes whether additional guidance is needed for particular patient or staff groups or whether reasonable adjustments are required to avoid negative impact on disabled patients, carers or staff.

Equality Analysis *Liaise with the Engagement Team if support is required at kchft.equality@nhs.net*

EQUALITY ANALYSIS

MONITORING COMPLIANCE AND EFFECTIVENESS OF THIS POLICY

- Line Managers will be responsible for ensuring individuals that handle patient identifiable information are aware of this policy

- Information sharing incidents must be reported immediately to the line manager via the Trust's online incident reporting system (known as "Datix"), as per the Trusts Incident Policy. Any such incidents whereby breaches of this policy have occurred will be investigated in liaison with the Performance Team

- The Information Governance Assurance Group (IGAG) will be responsible for leading on the implementation of this policy.

- This policy will be continually monitored and will be subject to regular review, which will take place every three years from the date of issue. The Performance Team will carry out the review and any changes will be ratified by the Information Governance Assurance Group.

An earlier review may be warranted if one or more of the following occurs:

- as a result of regulatory / statutory changes or developments
- as a result of NHS policy changes or developments
- for any other relevant or compelling reason

- KCHFT will work closely with the Audit Committee to assist in conducting audits across Community Health where breaches of this policy have arisen.

- An annual audit will take place of the pseudonymisation/anonymisation controls detailed in this policy.

- The audit will be carried out by an independent member of the Information Quality Assurance Group (IQAG)

- The audit will be conducted using the template in appendix 2.

- Results of the audit will be submitted as part of the annual IG toolkit and reported to the IQAG.

- Audits will take place in December/January each year, with the auditor decided at the IQAG meeting held prior to this date.

- Audit outcomes will be summarised and presented at the January IQAG and signed off.
- Summary will also be included in the Assistant Director of Performance and BI's report to the IGAG.

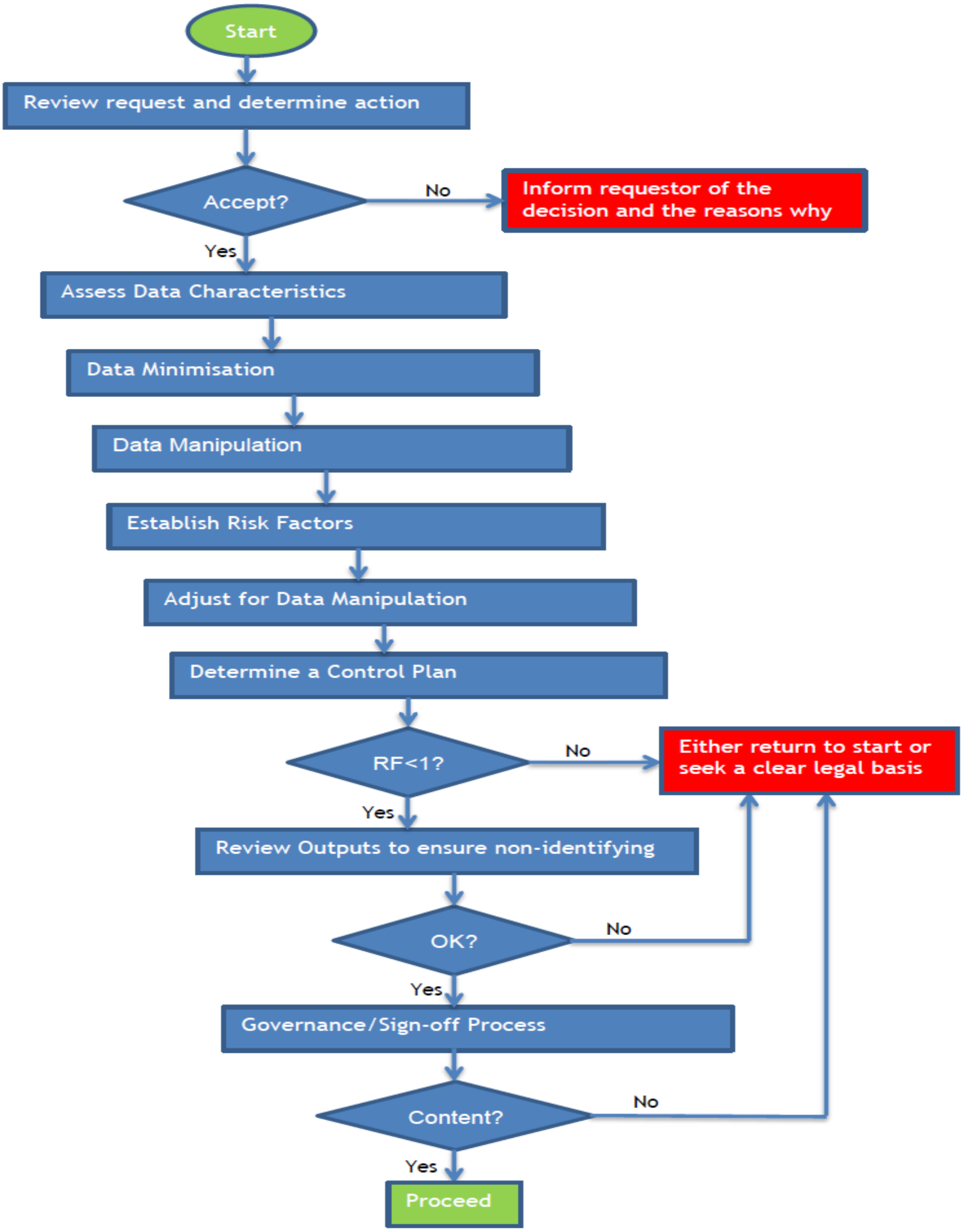
MONITORING MATRIX:

What will be monitored?	How will it be monitored?	Who will monitor?	Frequency
Audit of impact and compliance	Number of incidents and requests for IG advice	IG team	As part of daily routine
Staff awareness of the documents and associated requirements	Through annual IG training and line management process	Line managers to ensure mandatory training is updated and policy signature sheet is complete	Annually

GLOSSARY AND ABBREVIATIONS

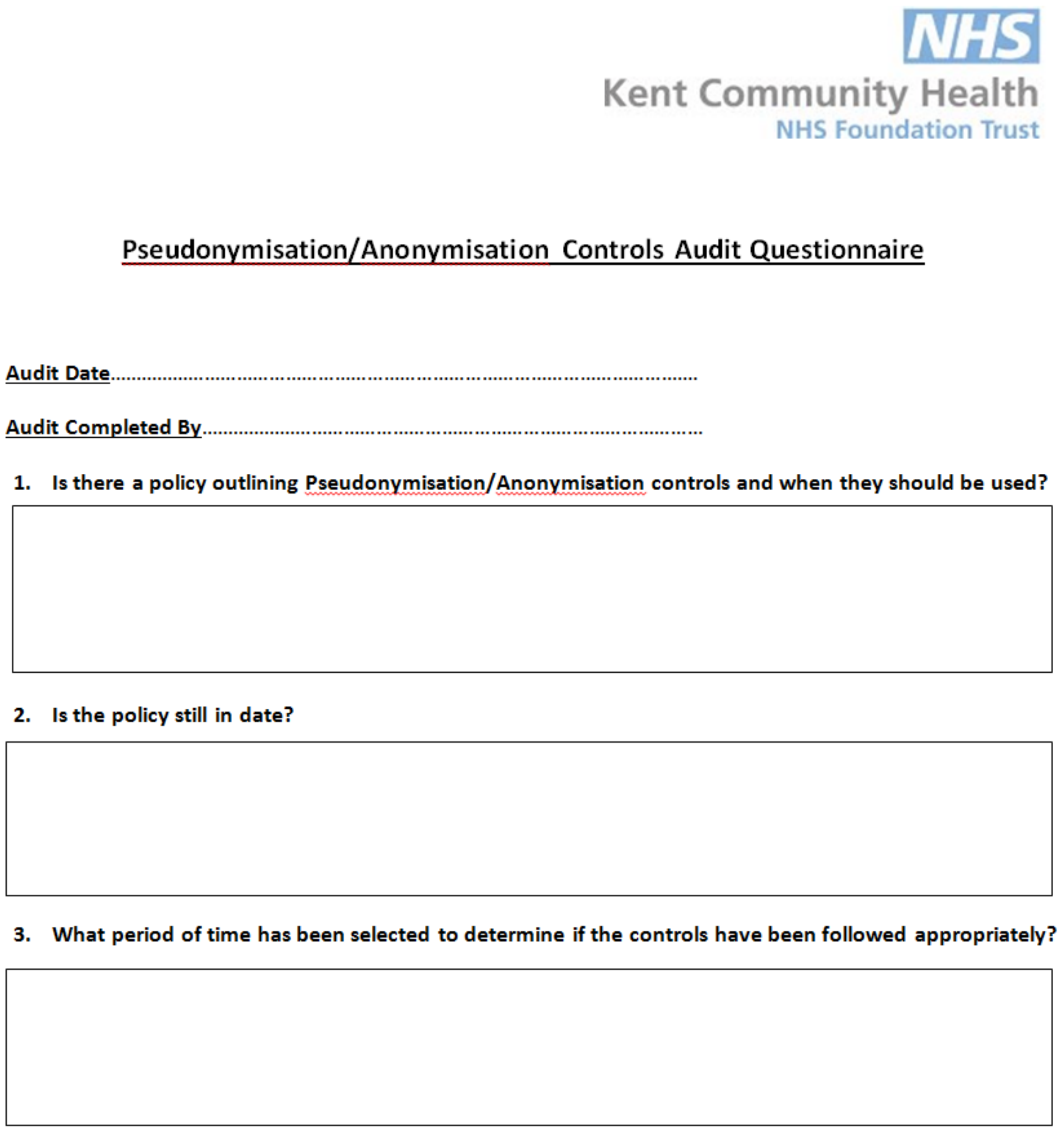
Abbreviation	Meaning
KCHFT	Kent Community Health NHS Foundation Trust
IGA	Information Governance Alliance
ICO	Information Commissioner’s Office
IGAG	Information Governance Assurance Group
IQAG	Information Quality Assurance Group
AIS	Accessible Information Standard
Anonymised Data	Data that has been turned into a form which does not identify individuals and where identification is not likely to take place.
Pseudonymised Data	Data where the most identifying fields within the dataset have been replaced with artificial identifiers, or pseudonyms. The purpose is to render the data record less identifiable and therefore reduce concerns with data sharing and data retention.
Secondary Use	The use of patient data for purposes other than direct or 'primary' clinical care

Appendix 1 – Anonymisation process Flowchart


Start
Review request and determine action
Accept?
No
Inform requestor of the decision and the reasons why
Yes
Assess Data Characteristics
Data Minimisation
Data Manipulation
Establish Risk Factors
Adjust for Data Manipulation
Determine a Control Plan
RF<1?
No
Either return to start or seek a clear legal basis
Yes
Review Outputs to ensure non-identifying
OK?
No
Yes
Governance/Sign-off Process
Content?
No
Yes
Proceed

Source (IGA Implementing the ICO Anonymisation Code of Practice: Guidance for Health & Care Services on disseminating data into controlled environments)

Appendix 2 – Pseudonymisation/Anonymisation audit template



NHS
Kent Community Health
NHS Foundation Trust

Pseudonymisation/Anonymisation Controls Audit Questionnaire

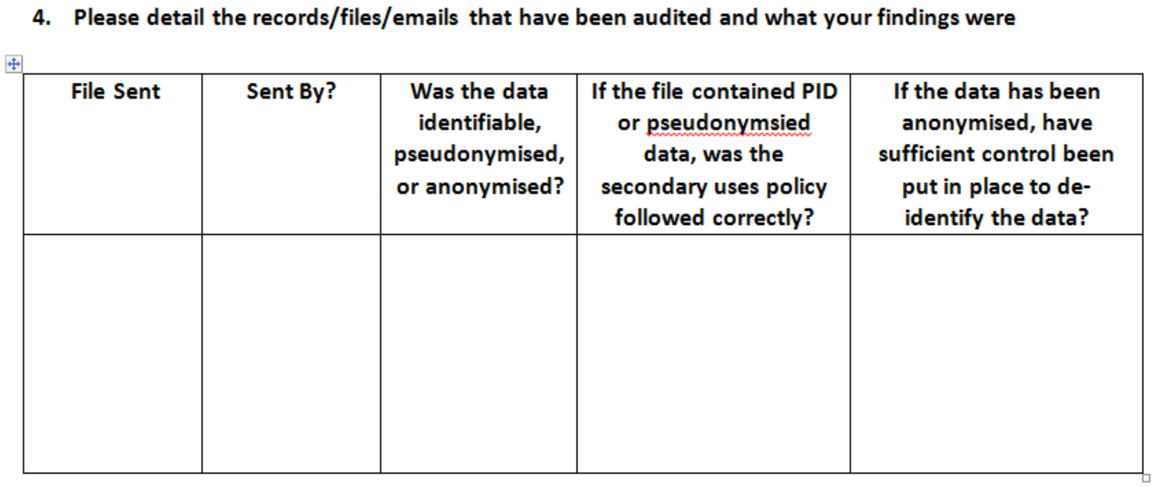
Audit Date……………………………………………………………………………………

Audit Completed By…………………………………………………………………………

1. **Is there a policy outlining Pseudonymisation/Anonymisation controls and when they should be used?**

2. **Is the policy still in date?**

3. **What period of time has been selected to determine if the controls have been followed appropriately?**



4. Please detail the records/files/emails that have been audited and what your findings were

File Sent	Sent By?	Was the data identifiable, pseudonymised, or anonymised?	If the file contained PID or pseudonymsied data, was the secondary uses policy followed correctly?	If the data has been anonymised, have sufficient control been put in place to de-identify the data?