Policy: Pseudonymisation and Anonymisation Policy

Author: Information Governance Team

Date: May 2021

Version: V1.0

GMCA GREATER MANCHESTER COMBINED AUTHORITY

GMCA, Churchgate House, 56 Oxford Street, Manchester, M1 6EU

Document Version Control

Document Type:	**Ref number**:
Document Name:	**Classification**:
Requirement for Document:	**Target Audience:**
Executive Summary:	
Executive Lead:	**Document Author:**
Ratified by/Approving Committee:	**Date Ratified**:
Date issued:	**Review Date:**
Circulation:	
Consultation:	
Superseded Documents:	**Cross Reference – Related policies and procedures:**
Date of Equality Impact Assessment:	**Date of DPIA:**
Contact Details for further information:	

Document Version

Version Date	Type of Change	Date	Revisions from previous issues	By

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

1.1 The Greater Manchester Combined Authority (GMCA) was established in April 2011 and since 2017 also has in place the elected Mayor of Greater Manchester who works collaboratively with other public sector organisations, voluntary and private enterprises in order to drive beneficial outcomes for the GM region and the lives of all its citizens. By encouraging economic growth, facilitating public sector reform, provision of a front-line fire and rescue service, Police and Crime Commissioner functions and delivering the Greater Manchester Strategy.

1.2 In order to fulfil its functions and duties as a Combined Authority the GMCA collects and processes personal data relating to individuals who use the services it provides, past, present and prospective employees, contractors, suppliers, clients, and others with whom it communicates.

1.3 The GMCA is responsible for being instrumental in the strategic changes required across GM to enable increased information sharing across public service delivery for public benefit. It is therefore imperative that organisational compliance with Data Protection laws for the GMCA is one that is continually striving for excellence.

1.4 As a public Authority the GMCA is obliged to comply with the UK General Data Protection Regulation[1] (UK GDPR) and the Data Protection Act 2018[2].Both of these pieces of legislation require the GMCA to process only the minimum amount of personal data needed for one or more specified purposes. Also to not use information that identifies individuals unless necessary.

1.5 The UK GDPR provides a set of principles to follow to handle personal data appropriately and in accordance with the law. The principle that supports the practice of only using the amount of personal data necessary is called the *'Data minimisation principle*' and is set out in Article 5(c) of GDPR. Data minimisation is also formally recognised in the third Caldicott[3] principle in relation to processing patient data and information, and it states: "Don't use personal confidential data unless it is absolutely necessary".

1.6 There are various ways in which data use can be minimized, where personal data isn't necessary for the purposes or the outcomes that are trying to be achieved, and so Pseudonymisation and/or anonymization techniques should be applied to the data.

[1] Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
[2] Data Protection Act 2018 (legislation.gov.uk)
[3] The Caldicott Principles - GOV.UK (www.gov.uk)

1.7 Effective pseudonymisation and/or anonymisation processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality. They are part of the Data Protection by Design[4] approach through which data protection is integrated into processing activities and business practices, from the design stage right through the lifecycle. They will often be relevant to a Data Protection Impact Assessment (DPIA) and form a key technical measure to ensure processing complies with the data protection principles.

1.8 This policy therefore sets out the commitment of how the GMCA will comply with the data minimisation principle and the use of pseudonymisation and anonymisation.

2. Policy Scope

2.1 This policy applies to all personal information including health data, special category/criminal conviction data used, stored or shared by or with the GMCA whether in paper or digital form and wherever it is located. It also applies to all personal information and special category information processed by the GMCA on behalf of other organisations

2.2 This policy applies to all GMCA employees, seconded staff members, volunteers, third party contractors, temporary staff and employees of other organisations who directly or indirectly support GMCA services.

2.3 This policy applies to data processing where the GMCA is a data controller in its own right or is a data controller in relation to a multi-agency data sharing partnership. This policy also applies when the GMCA is acting as a Data processor on behalf of one or more data controllers

3. Policy Statement

3.1 This policy states how the GMCA will comply with the GDPR's data minimization principle using anonymisation and pseudonymization techniques

3.2 As the GMCA processes a wide range of information this policy does not provide detailed guidance on the application of anonymisation and pseudonymization techniques or individual areas of application; these will be captured within the supporting procedural documents.

[4] Data protection by design and default | ICO

4. Roles and Responsibilities

4.1 Chief Executive

The Chief Executive is responsible for the organisation's compliance with data protection legislation. Part 7 of the DPA 2018 stipulates the CEX's liability with regards to offences committed under the Act.

The Chief Executive is therefore ultimately responsible for ensuring the GMCA only processes personal identifiable data where necessary and complies with data minimization principles.

4.2. Monitoring Officer

The Monitoring Officer is responsible for ensuring the lawfulness and fairness of GMCA decision making and must report on matters they believe are, or are likely to be, illegal or amount to maladministration. They are also responsible for matters relating to the conduct of members and officers. The GMCA Solicitor is the Monitoring Officer

4.3 Senior Information Risk Owner (SIRO)

The SIRO has an overall strategic responsibility for governance in relation to data protection risks and is responsible for:

- Acting as an advocate for managing information risk within the GMCA championing and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs.
- Providing written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk.

4.4. Data Protection Officer (DPO)

Under the Data Protection Legislation all public authorities must appoint a DPO. The DPO is responsible for:

- Informing and advising the GMCA and its employees of their data protection obligations.
- Monitoring compliance with the Data Protection legislation and internal data protection policies and procedures.

- Monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Acting as the contact point for the supervisory authority (Information Commissioners Office) on all data protection issues, including data breach reporting.

The GMCA will meets its obligations regarding the DPO role and as such will ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, i.e. board level at the GMCA this is the SIRO;
- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) is provided to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;
- The DPO has the appropriate access to personal data and processing activities;
- appropriate access to other services within your organisation so that they can receive essential support, input or information.

The Data Protection Officer for the GMCA is the Assistant Director of Information Governance.

4.5. Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are members of the Extended Leadership Team. Their role is to understand in their business area what information is held, what is added and what is removed, how information is moved, and who has access and why. The IAO is responsible for:

- ensuring they are understand and address risks to the information.
- ensure that information is fully used within the law for the public good.
- providing a written judgement of the security and use of their asset annually to support the audit process.
- ensuring their business area complies with the data minimisation principle
- to consider pseudonymisation and anonymisation techniques at the project initiation stage, as part of the DPIA process

4.6. Information Asset Administrators (IAA)

An IAO is accountable for the information assets under their control but may delegate day to day management responsibility to an IAA who would be responsible for:

- Ensuring all team members keep their training up-to-date
- Supporting the IAO by ensuring their business area complies with the data minimisation principle and the use of pseudonymisation and anonymisation

4.7. Information Security Officer

The Information Security Officer is responsible for developing and implementing the GMCA Information Security and associated policies and procedures to reflect local and national standards and guidance and legislative requirements. They also support the GMCA in ensuring compliance with information security requirements. This role reports to the Deputy Chief Information Officer.

4.8. Heads of Department will:

- Ensure all managers are made aware of this policy and understand their duties to ensure compliance across their teams.
- Notify the Information Governance Team and seek advice where activities involve the use of personal data. This includes any new projects, new data processing or any changes to existing processing
- Ensure compliance with GDPR and Data Protection Legislation for all teams within their area.
- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum complete the GMCA's data protection training every year.
- ensure their business area complies with the data minimisation principle and the use of pseudonymisation and anonymisation techniques to remove personal identifiers from the processing of information where appropriate.

4.9. Line managers will:

- Ensure that their teams are made aware of this policy and understand its requirements.
- Fully implement the requirements of this policy within their teams.
- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum GMCA's data protection training every year.
- Ensure the data they're responsible for is anonymized or pseudonymised where it is appropriate to do so.
- Ensuring all breaches or suspected breaches of confidentiality or information security are reported for immediate investigation. In particular, this includes the unauthorised reversal of pseudonymisation.

4.10. All staff must:

- All staff who create, receive and use personal information including health data, special category or criminal conviction data have pseudonymisation and anonymisation responsibilities under the Data Protection Act and supporting information governance policies.
- Follow this policy for all processing of personal data throughout the GMCA.
- Protect any personal data within their care.

- Seek additional advice and guidance from their manager, Information Governance Team or the Data Protection Officer if unsure or in any doubt about how to handle personal information.
- Report any suspected or actual data breaches or any breaches of this policy to their line manager or the Information Governance team as soon as they become aware in line with the Serious Information Governance Incident procedure.
- Keep up to date with all GMCA Data Protection and Information Governance training that is appropriate to their role
- Ensuring all breaches or suspected breaches of confidentiality or information security are reported for immediate investigation. In particular, this includes the unauthorised reversal of pseudonymisation.

4.11. Information Governance Team will:

- Will be the source of subject matter expertise in relation to data protection Develop and inform strategies in relation to the use of personal data
- Provide strategic oversight to large scale programmes of personal data sharing
- Will advise on and provide support in relation to data protection and the handling and use of personal data.
- Will provide guidance and support to staff undertaking Data Protection Impact Assessments.
- Develop and maintain relevant policies and procedures in line with changes to legislation and best practice.
- Manage and monitor requests from Data Subjects who choose to exercise their individual rights including Subject Access Requests in line with GMCA policies and procedures.
- Manage and monitor any Information Security Breaches in line with the GMCA Information Security Breach Policy.
- Develop and deliver training as required.

5. Definitions

5.1 **Personal Data -** Any information relating to a natural person who can be identified directly from the information or could be in combination with other information.

5.2 **Anonymisation -** The process of turning data into a form which does not identify individuals and where identification is not likely to take place. Anonymisation describes the process of data de-identification, producing de-identified data that cannot be linked to the original source or to an individual**.**

5.3 **Anonymised Data -** Data in a form that does not identify individuals and where identification through its combination with other data is unable to take place.

5.4 **De-identification -** The de-identification of data refers to the process of removing or obscuring any personally identifiable information from records in a way that minimises the risk of unintended disclosure of the identity of individuals and

information about them. Methods used to de-identify information may vary depending on the circumstances but should be appropriate to protect the confidentiality of the individuals and the intended secondary use of the data.

5.5 **Pseudonymisation -** This is a method of removing the identifiable nature of data by using a unique identifier which does not reveal their 'real world' identity. In order to de-identify the data a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified. The ICO draws a distinction between anonymisation techniques used to produce aggregated information and those such as pseudonymisation that produce anonymised data but on an individual-level basis.

Data Protection legislation supports the use of pseudonymisation as an appropriate safeguard where anonymisation is not practical, yet it should be recognised that data that has undergone pseudonymisation can still be considered information about an identifiable natural person.

5.6 **Pseudonym -** This is a coded reference used to conceal/de-identify the personal data. This reference can be stored securely in order to re-identify the data back to its original form if necessary.

5.7 **Aggregation –** The merging of data to present figures in a way which does not allow the identification of individuals. This is where data are displayed as totals, so no data relating to or identifying any individual is shown. Small numbers in totals are often suppressed through 'blurring' or by being omitted altogether. Consolidating

6. Anonymisation and Pseudonymisation principles

6.1 Data Protection legislation classifies pseudonymised data as personal data and therefore must be processed in accordance with all data protection legislation. If the GMCA has access to the pseudonymised data and the identifiable personal confidential data; the key to the pseudonym; or has the means to re-identify pseudonymised data, the pseudonymised data remain in scope for full compliance with data protection legislation.

6.2 Data protection legislation states that data which is truly anonymised in such a way that individuals cannot be identified or re identified does not fall within the scope of the UK GDPR and therefore does not fall within the scope of the Data Protection Act either.

6.3 It is always preferable to fully anonymise any data that has the potential to reveal something personal about an individual, either from that data alone or when combined with other data.

6.4 Where data cannot be used in an anonymised format, due to the need to link datasets, because data may ultimately need to be re-identified or processed in identifiable format, the personal or data or pseudonymised data may be used

provided there are strict controls in place to prevent unauthorised access and unauthorised re-identification.

6.5 The key advantages of using anonymised data as opposed to identifiable data include:

- it is easier to use anonymised data in new and different ways because the data protection legislation “purpose limitation rules do not apply;
- protection against unauthorised access or disclosure of personal data; fewer legal restrictions apply;
- allow for the sharing of data with colleagues and teams for analysis
- allows organisations to make information public while still complying with their data protection obligations; and
- the disclosure of anonymised data is not a disclosure of personal data.

6.6 The GMCA will carry out a thorough risk analysis on the likelihood and potential consequences of re-identification at the initial stage of producing and disclosing anonymised or pseudonymised data. The GMCA will always use a DPIA (Data Protection Impact Assessment) to undertake this assessment of risk, in line with Article 35 of GDPR.

6.7 The risk of re-identification will differ according to the way the anonymised or pseudonymised information is disclosed, shared or published. Publication to the wider public would be considered far more risky than limited access.

6.8 Any pseudonymization and anonymisation techniques used in GMCA projects must therefore be employed as part of a ‘holistic methodology’ of technical and non-technical processes to protect personal data enshrined in the concept of privacy by design and default (Article 25).

7. Anonymisation

7.1 The organisation will use de-identification and anonymisation techniques to obscure or remove the identifiable data items within a person’s records sufficiently that the risk of potential identification of the subject or a person’s record is minimised to acceptable levels, so as to provide effective anonymisation, where appropriate. Recital 26 of GDPR defines anonymous information, as "…information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". The GDPR does not apply to anonymised information as set out above in Section 6.

7.2 Anonymised data will allow information which originated as personal confidential data to be available in a form that is rich and usable, whilst protecting the confidentiality of the individual.

7.3 The organisation will continue to comply with role-based access controls when using de-identified and anonymised data.

The organisation will achieve de-identification and anonymisation by:

- Removing personal identifiers (e.g. name, date of birth, physical description etc)
- The use of identifier ranges, for example; value ranges instead of age.
- Aggregation.
- Using a pseudonym (although, as covered further below, pseudonymising data will not necessarily completely ensure that re-identification is impossible).

The organisation will ensure that any commissioning and contracting on behalf of the GMCA will include assurances that the Provider's processes are robust in respect of the supply of data and data minimization principles.

The most up to date guidance from the Information Commissioners Office on Anonymisation can be viewed here; https://ico.org.uk/media/1061/anonymisation-code.pdf

8. Pseudonymisation

8.1 Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being. Essentially this means substituting the identifiable part of the data with something else, in a way that the data can only be re-identified using a key for example.

The GMCA will effectively pseudonymise data by:

- Removing personal identifiers and ensuring Personal Identifiable Data is replaced with a unique pseudonym;
- When using pseudonymisation externally, it's important to use different pseudonyms internally, such that internal data use/processes are not compromised;
- Pseudonymised data will have the same security applied to it as all other Personal Identifiable Data

10. Legal and Professional Obligations

10.1 The GMCA will take actions to comply with the relevant legal and professional obligations, in particular:

- General Data Protection Regulation and Data Protection Act 2018

- Human Rights Act 1998
- Common Law Duty of Confidentiality
- The Information Commissioner's Office (ICO) code: anonymisation: managing data protection risk code of practice
- NHS Digital Data Security and Protection Toolkit

11. Training

11.1 The GMCA will provide relevant training both on line and face to face to ensure that staff understand the legislation and its application to their role.

11.2 All staff must complete mandatory data protection training every year and undertake any further training provided by the GMCA to enable them to perform their duties appropriately

12. Compliance and Monitoring

12.1 Completion of training will be monitored by the Information Governance Team and all employees must have regard to the Data Protection Legislation and this policy when collecting, accessing, using, disclosing or destroying personal information. Failure to do so may result in disciplinary action and legal prosecution.

12.2 If an employee is in any doubt about how to handle personal information or to apply the pseudonymisation/anonymisation techniques mentioned above, they should speak to their line manager or contact the Information Governance Team OfficeofDPO@greatermanchester-ca.gov.uk

12.3 This policy will be reviewed at regularly by the Information Governance Team to ensure that it is updated in line with any change in legislation.

12.4 The GMCA will continue to review this effectiveness of this policy to ensure that it is achieving it intended purpose.

Appendices

Appendix 1: Related Policies and Procedures

- GMCA Information Disclosure Policy.
- GMCA Information Security Policy
- GMCA Records Retention Policy
- GMCA Data Quality Policy
- GMCA Subject Access Policy
- GMCA Disciplinary Policy
- GMCA Employee Code of Conduct
- GMCA Freedom of Information Act Policy

Appendix 2 Further Information and Guidance

Data Protection Officer

Data Protection Officer – Assistant Director Information Governance

GMCA, Churchgate House, 10, Oxford Street, Manchester M16EU

Email: OfficeofDPO@greatermanchester-ca.gov.uk

Information Commissioner

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Tel: 0303 123 1113

www.ico.org.uk

On line Resources

- ICO – www.ico.org.uk
- GMCA intranet