

Data Subject Rights Policy

IG03 Information Governance

August 2024

**Contents**

[1 Introduction 2](#_Toc174706655)

[2 Scope and Purpose 2](#_Toc174706656)

[3 Definitions 2](#_Toc174706657)

[4 Proof of identity 5](#_Toc174706658)

[5 Time frame for processing the request 6](#_Toc174706659)

[6 The right to be informed 6](#_Toc174706660)

[7 The right of access 7](#_Toc174706661)

[8 Right to rectification 15](#_Toc174706669)

[9 Right to erasure 15](#_Toc174706670)

[10 Right to restrict processing 15](#_Toc174706671)

[11 Right to data portability 16](#_Toc174706672)

[12 Right to object 16](#_Toc174706673)

[13 Rights in relation to automated decision making and profiling 16](#_Toc174706674)

[14 Roles and Responsibilities 17](#_Toc174706675)

[15 Training and Monitoring 20](#_Toc174706676)

[16 Communication and Dissemination 20](#_Toc174706677)

[17 Resources 21](#_Toc174706678)

[18 Version Control 21](#_Toc174706679)

1. Introduction
   1. MHA is committed to processing personal data in accordance with the Legislation. Data Subjects have rights which must be processed within 1 calendar month. This policy details these rights and how they should be applied.
2. Scope and Purpose
   1. All MHA colleagues and third-party organisations that process Personal Data for or on behalf of MHA, are required to:
   * Ensure that all colleagues are aware of their roles, responsibilities and accountability and fully comply with the Legislation as described in this and other Information Governance policies.
   * Create and maintain a level of awareness of the need for confidentiality and information security as an integral part of MHA’s day to day business.
   * Protect information assets under MHA’s control.
3. Definitions

| Term | Definition |
| --- | --- |
| **Colleagues** | A Data Subject who works part-time or full-time for MHA under a contract of employment (staff), volunteer agreement (volunteer) or as an independent contractor. |
| **Data Controller** | The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; |
| **Data Processor** | A natural or legal person, or third-party which processes personal data on behalf of the Data Controller. |
| **Data Protection Legislation,**  **Legislation** | This includes: the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR) as updated from time to time. |
| **Data Subject** | An Identifiable living individual. For MHA this is past & present, living: colleagues, residents, family members and supporters or any person for whom MHA processed or has processed personal data |
| **Document**  **(see Record)** | A piece of writing that contains information, e.g. a recipe. |
| **IT Policy** | The IT policy Computer Use Policy and IT guidance, which may be updated from time to time. |
| **Legal Hold (or Litigation Hold)** | The need to ensure that documents, relevant to the subject matter of a pending or anticipated lawsuit, investigation, or inquiry, are kept safe from being edited, deleted, or destroyed. |
| **Personal Data** | Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person |
| **Process, Processed, Processing** | Any operation or set of operations performed on Personal Data or on sets of Personal Data, by automated or manual means. Operations may include collect, record, organise, sort, store, edit, retrieve, use, disclose, combine, restrict, erasure, or destroy. |
| **Record**  **(see Document)** | A piece of writing that contains information that can be used as evidence, e.g. that a recipe was followed on a specific date, food temperatures were checked, food was served to x, y & z. |

1. Proof of identity
   1. Before taking action on any requests regarding the rights of Data Subjects it may be necessary to verify the requester’s identity. If the request is made in person, i.e. face to face with a colleague, and the person is known there is no need to ask for proof of ID. Proof of ID may be necessary if:
   * The request is received over the phone and the identity of the caller is unsure. A statement from the caller saying, “I am [first name] [last name]” is not sufficient. You must be confident you recognise the voice or ask for additional information, e.g. their date of birth or their home address, checking the answer are correct.
   * The request is made from an email address that has never been used before, even if it is in their name.
   * The request is made via the post.
   * The request is made in person, i.e. face to face with a colleague, but the person is not known to the colleague.
   1. Suitable forms of ID are:
   * A copy of their photo driving license, or
   * A copy of the photo page of their passport and proof of address dated within the last 3 months on official paper - e.g. bank statement, utility bill or council tax bill.
   * If a telephone request if made by an NHS or locally authority representative, then an email from them is an acceptable form of ID if it is from their business email address. Note: This is not because we need the request in writing, it is to affirm they work for the NHS or local authority.
   1. Once the identity is suitably confirmed the one calendar month for processing starts. Log the forms of identification, recording the last four digits of any license, passport or account number. Destroy any paperwork unless it was requested that it be returned.

**NOTE:** The destruction only relates to ID documents for this purpose, not for documents requested for Right to Work.

1. Time frame for processing the request
   1. The Legislation requires that the request is completed within one calendar month of the request being received, if no proof of ID is required. If proof of ID is required it should be completed within one calendar month of the proof of ID being received.
   2. If proof of ID is required, but is not requested promptly, then the delay must be taken into account when determining the date by which the request must be completed.
   3. In some circumstances it may be possible to extend the processing time by two months, if the request is large and/or complex. This will be determined by the DPO.
2. The right to be informed
   1. Privacy Notices must be provided at the point that the data subject provides their data to MHA. Where possible notices should be provided using the same media as the data collection.
   * **In person:** offer a paper copy or direct them to the website.
   * **Post**: send a paper copy or the web address as appropriate.
   * **Email:** Include a link to the web address.
   * **Phone:** A summary can be provided over the phone, but full notice should be offered by post or email.
   1. Privacy Notices explain:
3. what data is held,
4. the source of the data if not from the Data Subject,
5. how it will be used,
6. the legal basis for holding it,
7. if it will be shared,
8. how it will be kept secure,
9. how long the data will be kept,
10. a summary of these rights
11. contact details of the Information Commissioner’s Office and the DPO.
    1. The DPO is responsible for maintaining the Privacy Notices, which will be updated from time to time. The latest versions are available on MHA’s intranet and website (www.mha.org.uk/PrivacyPolicy).
    2. MHA provides Privacy Notices covering all aspects of data processing for our Data Subjects. These include (most of this should be covered by the Privacy Notices):
12. Colleagues (contractors, employees & volunteers)
13. Residents and Tenants (care home & retirement living)
14. MHA Communities Members
15. Relatives
16. Supporters (including donors and fundraisers
17. Website
18. Property Sales and letting
19. Mobile Phones
20. The right of access
    1. The “right of access” is more commonly known as a “Subject Access Request” (SAR).
    2. Data Subjects are entitled to obtain the following information about their own Personal Data:
21. The purposes of the collection, processing, use and storage of their personal data.
22. The source(s) of the personal data, if it was not obtained from the Data Subject.
23. The categories of personal data stored for the Data Subject.
24. The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients.
25. The envisaged period of storage for the personal data or the rationale for determining the storage period.
26. The use of any automated decision-making, including profiling.
    1. In addition to the above the Data Subjects have the right to view or request copies of the data that relates to them.
    2. SARs can be made by the Data Subject or a third party. All SARs, whether received in writing or verbally, must be reported to the DPO. The DPO will log and as necessary, assist with the provision of the requested information. There are exemptions to the need for authorisation that may need to be considered (see 7.10.6).
    3. If records are being viewed, the viewing must take place in the presence of a staff member. Records should not be left unsupervised. It is not permissible for photos of records to be taken, e.g. with a mobile phone. If copies are required inform the DPO.

Information that must NOT be provided as part of a SAR

* 1. The Legislation provides several exemptions, regarding information that should not be provided as part of a SAR. Information should not be provided if:
  + It relates to a confidential employment reference.
  + It is likely to cause serious physical or mental harm to the patient or another person.
  + It relates to a third party who has not given consent for disclosure and the DPO concludes it is reasonable to withhold third party information.
  + It is requested by a third party and the Data Subject had asked that the information be kept confidential, or
  + It is restricted by order of the courts.

Information to pass to the DPO

* + 1. When a request for access to records is received, the DPO is required by law to log all requests. The following must be provided to the DPO:

1. The date the request was received
2. The full name of the Data Subject – resident, colleague, etc.
3. The full name individual making the request if not from the Data Subject.
4. Contact details of where the records are to be sent: address or email address.
5. Details of what is being requested. Ideally a copy of the request: email, scanned letter or record of a verbal request.
6. The date the records were provided

The DPO will log the request and either:

* + provide instruction on the provision of the information, or
  + handle all communication and the provision of the information. The information will need to be provided to the DPO in a timely manner so that the legal timeframe of 1 calendar month can be achieved.

Business as Usual Requests

* + 1. Business as usual requests cover requests for information that we are: either contracted to provide, legally required to provide or would reasonably be expected to be provided.
    2. If you believe additional requests for records should be deemed BAU please inform the DPO, who will consider the request.
    3. These can be processed by the MHA service receiving the request as long as the referenced policy has been followed.
    4. These fall into two categories:

DPO must be informed

* + - 1. DPO must be sent:

1. The date the request was received
2. The full name of the Data Subject – resident, colleague, etc.
3. The full name individual making the request if not from the Data Subject.
4. Contact details of where the records are to be sent: address or email address.
5. Details of what is being requested. Ideally a copy of the request: email, scanned letter or record of a verbal request.
6. The date the records were provided
   * + 1. Types of BAU requests where information must be sent to the DPO:
   * Requests for resident’s records from the NHS or local authority for: direct care, a CHC assessment or resident’s care review
   * Records to support a DoLS request
   * Records relating to a safeguarding event
   * Requests from a Coroner (whether about a deceased resident or a colleague)

DPO does not need to be informed

* + - 1. The request and the information must be recorded in the appropriate file, e.g. resident’s file or HR records/Personal File (paper or electronic).
      2. BAU requests - details don’t need to be sent to the DPO:
  + Request to view or for a copy of a specific HR record that the colleague would be expected to have a copy of, e.g. payslip, P60, 1:1 or appraisal records, training records or certificates. If the request asks for the whole personal file this is not a BAU request.
  + Request for an employment reference (see HR9.12)
    - 1. If you are in doubt, or unsure, please contact the DPO.

SARs made by third parties

* + 1. In addition to the Data Subject making a request other individuals or parties can make requests. In each situation there needs to be an appropriate authorisation to disclose the records. This will typically be signed consent from the Data Subject, their registered attorney or court appointed deputy.

Power of Attorney (PoA) and Deputyship

* + - 1. The process to validate and check the Attorney and Deputyship is explained in MHA’s Mental Capacity And Deprivation Of Liberty Safeguards Policy, section 7.
      2. A Health and Welfare Attorney can make decision on the care provided to the donor so has access to the care records.
      3. The ICO has stated that where an individual does not have the capacity to make a decision regarding a Subject Access Request for care records, “it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority”. MHA has interpreted this to also mean that to make a decision on whether to authorise a SAR that they must know the contents of the records. Therefore, all Attorneys and Deputies are granted access to records and have the authority to authorise SARs.
      4. Once the donor dies the PoA or Deputyship automatically ends.

Family members and Next of Kin

* + - 1. Family members and Next of Kin do not automatically have access to care records. A resident with capacity can complete the Nominated Individual’s Consent Form. This allows the resident to detail who should have access to their financial and/or care records and information. This decision would remain valid after capacity is lost or until an Attorney or Deputy is registered.
      2. If there is no LPA, Deputy or completed the Nominated Individual Form and the resident does not have capacity to complete the form, a Best Interest Assessment must be completed.

Healthcare Professionals (incl. NHS) and Social Workers

See 7.9 BAU requests.

Lawyers

* + - 1. Lawyers are typically acting for an individual and need to provide authorisation from the individual for the requested records to be provided.

Research Requests (incl. National Data Opt-Out)

* + - 1. MHA must not share confidential personal data for research purposes, unless explicit consent has been given. Therefore, MHA does not need to review resident’s National Data Opt-Out status.

Exemptions to the need for authorisation

* + - 1. The Legislation provides exemptions for the need of authorisation for records to be provided. This means that in specific situations third parties can request copies of records without consent or authorisation from the Data Subject, and possibly with a requirement that the Data Subject is not made aware of the request:

1. **Crime and Taxation:** The Legislation exempts MHA from needing consent from the Data Subject when providing personal data regarding a crime (e.g. to the police) or taxation (e.g. to the HMRC or Council Tax Office). Before any information is provided an official request must be submitted.
2. **Legal Proceedings:** The Legislation exempts MHA from needing consent from the Data Subject where disclosure of the personal data is required for legal proceedings or possible legal proceedings. Such requests are likely to be received from solicitors acting for an individual or Insurances companies relating to a claim.
3. **Safeguarding (including DoLS):** A Safeguarding team may request information regarding a resident in relation to a safeguarding incident or a complaint, or about a staff member involved in an incident.
   * + 1. The DPO must be informed of all requests. The DPO will log the request and ensure the request is completed. The records may need redacting to protect other individuals identified in the documents.
       2. If the request is made verbally an email or written confirmation should be requested, so we have a record of the request and to aid proof of ID of the requester. Where no written confirmation is provided MHA has templates to be completed and signed when the records are collected. These must be sent to the DPO when signed (see appendices).

Regulatory or Statutory Exemptions

* + - 1. In addition to the exemptions mentioned above, there are a number of regulatory and statutory exemptions:
  + CQC (and other Regulators – CIW, CIS).
  + Nursing and Midwifery Council (NMC).
  + Coroner – a coroner can request records beyond those of the deceased.
  + Care Quality Commission (CQC) (and other Regulators – CIW, CIS)
    - 1. In order to exercise these powers, the representative must hold a duly authenticated document showing they have been granted these powers or make the request from an official email address.
      2. They can typically request any records they deem relevant.

Redacting Records

* + 1. MHA has a responsibility to protect other individuals that may be mentioned in the requested information. This will require that the documents are redacted so that no other individual can be identified - i.e. remove names, job titles, mobile phone numbers, direct dial numbers, or details that could identify the individual, etc.
    2. If care records are being provided to support the provision of care, then staff details do not need to be redacted.
    3. If a paper copy needs redacting: copy, redact and copy the redacted copy. It is often possible to read through black marker pen, photocopying resolves this.
    4. The protection of other individuals is also necessary when the Data Subject is granted access to view records - e.g. a staff member may want to view the personal file, or a resident may want to see their care records. If the file contains other identifiable individuals a redacted copy may need to be made available for viewing.

**NOTE:** The black highlighting features in Word and Adobe Acrobat are not redaction tools. These **must not** be used for redaction. The highlighted text can be selected, copied, and pasted - revealing the ‘redacted’ information.

How records are to be provided

* + 1. If the SAR, requesting a copy of the information held by MHA, was received by email and didn’t specify a paper copy, then the requested information should be provided in a password protected, commonly used, electronic format.
    2. If providing password protected Word or Excel files, ensure that only the request information is provided:
  + Delete any hidden data, rows or columns
  + Don’t highlight in black to hide data. See 7.11.5 Redacting Records.
  + Check the document properties to ensure no personal or business data is provided.
    1. If in doubt: print, scan to email, then password protect the PDF files, then email.
    2. If records are being viewed, the viewing must take place in the presence of a staff member. Records must not be left unsupervised. It is not permissible for photos of records to be taken, e.g. with a mobile phone. If copies are required inform the DPO.
    3. If information is to be sent by email, a secure system should be used unless sending to an @NHS.net or local authority (@\_\_\_.gov.uk) email address. E.g., password protect the PDF file or send a OneDrive password protected link.
    4. If records are to be posted, a ‘sign-for’ service must be used.
    5. If records are to be collected in person a signed receipt must be obtained. Templates have been created to facilitate this.

Repetitive or Excessive Subject Access Requests

* + 1. The DPA allows for a ‘reasonable fee based on administrative costs’ to be charged for repetitive or excessive requests. This has been calculated to be 27p per double sided page and 16p per single sided page, plus postage (typically about £10). The charge will be capped at £250.
    2. A cheque made payable to ‘Methodist Homes’ should be sent to:

Data Protection Officer, Methodist Homes,

Epworth House, Stuart Street, Derby, DE1 2EQ.

1. Right to rectification
   1. Data Subjects have the right to require MHA to correct or supplement erroneous, misleading, outdated, or incomplete personal data – e.g. correcting a misspelt name, change of mobile phone number.
   2. A right for rectification must be completed within one calendar month.
2. Right to erasure
   1. Data Subjects have the right to erasure (the right to be forgotten), to request that all the personal data they provided to MHA, be deleted. For example, a Data Subject could request that all entries relating to them on our social media and web sites be removed or could request that photos of them be deleted from MHA’s systems and no longer used in publications where consent was provided.
   2. The right to erasure is not absolute. If MHA has a reason to retain the information this may override the request, e.g. we may need to retain information after a financial gift.
   3. A right to erasure must be completed within one calendar month.
3. Right to restrict processing
   1. The Data Subject has the right to restrict processing of their personal data if they suspect that their personal data is incorrect, being processed beyond the original intention or MHA no longer need to hold the data - e.g. retention period has passed. All processing of their data must be stopped immediately until the issue is resolved to the Data Subject’s satisfaction.
   2. The restriction must stay in place until the reason for the restriction has been investigated.
   3. The restriction must not be lifted without informing the individual.
   4. The right to restrict processing must be implemented within one calendar month. The investigation and resolution must be completed within one calendar month.
4. Right to data portability
   1. The Data Subject has the right to request that personal information which they provided and is stored electronically, be exported into a universal format so it can be imported into another system.
   * The right does not apply to the records that MHA create.
   * The right to data portability must be completed within one calendar month.
5. Right to object
   1. The Data Subject has the right to object to processing of their personal data:
   * That is being processed under the lawful basis of legitimate interest or public interest, including profiling within this processing, or
   * for marketing purposes.
   1. As soon as the objection is received all processing must stop unless MHA can demonstrate compelling legitimate grounds for the processing which override their interests.
6. Rights in relation to automated decision making and profiling
   1. Data Subjects need to be informed of automated decision making and profiling processes and have the right to ask for their information to be processed in person. For example, applicants must be informed, prior to the processing, of any automated process to review and filter job applications.
   2. One receipt of the objection the processing must be carried out by a person.
   3. The right to have their data processed by a person must be completed within one calendar month of the request being received.
7. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **All Colleagues** | All colleagues must understand and apply to the Information Governance policies. |
| **Senior Managers** | Shall be individually responsible for the security of their physical environments where information is processed or stored. They are responsible for:   1. Ensuring that their team are aware of the information security policies, procedures, and user obligations applicable to their area of work. 2. Determining the level of access to be granted to specific individuals. 3. Ensuring colleagues have appropriate training for the systems they are using. 4. Ensuring that any data breaches are reported to the Data Protection Officer. |
| **Information Asset Owners (IAO)** | An information asset is any piece or collection of information stored by MHA and processed as a single unit - e.g. colleagues’ personal file, resident’s care record. It is something we can’t replace without cost, time, skill, and resources.  All service managers (CH, RL & MHA Communities) are IAOs. All department heads are IAO. IAOs are responsible and accountable for the security and processing of all their information assets, they will:   1. Lead and foster a culture that values, protects, and uses the information assets lawfully. 2. Know who has access to the assets, and why, ensuring use is monitored and compliant with policy. 3. Understand and address risks to the asset and provide assurance to the SIRO. 4. Ensure there is a lawful basis for processing and for any disclosures.   Maintain adequate records the assets that are processed. |
| **Head of Talent Acquisition and Shared Services** | The Head of Talent Acquisition and Shared Services is responsible for ensuring that the contracts of all colleagues (permanent and temporary) are compliant with the requirements of information governance and that data protection is included in inductions. |
| **Associate Director of IT** | 1. Develop IT policies that implement best business practice, ensuring they are applied throughout the business. 2. Ensure effective management and security of MHA’s IT infrastructure and equipment. 3. Responsible for and being the point of contact for IT security within MHA. 4. Monitoring potential and actual security breaches, informing the DPO as appropriate. 5. Develop and implement an IT Disaster Recovery Plan. |
| **Caldicott Guardian** | 1. The **Senior Nurse Advisor** is the Caldicott Guardian for MHA. The Caldicott Guardian will: 2. Work alongside the DPO to make sure that the personal information about people who use MHAs services is used legally, ethically, and appropriately and that confidentiality is maintained in relation to the storage, management and sharing of this information. 3. Provide leadership and informed guidance on complex matters involving confidentiality and information sharing regarding personal information for MHA’s residents. 4. Play a key role in ensuring that MHA satisfies the highest practical standards for handling the person information of people receiving care and support from MHA. 5. Apply the eight Caldicott Guardian Principles 6. Act as the conscience of MHA, providing impartial and independent advice. 7. Represent and champion information governance requirements and issues at senior management team and board level where appropriate, being and integral part of the overall information governance framework. 8. Play a key role in advising and ensuring that the Caldicott Principles are applied in digital and paperless systems. |
| **Data Protection Officer (DPO)** | MHA will ensure that there is always one person with overall responsibility for data protection, the DPO.  The DPO will:   1. Implement policies and procedures to embed the data protection principles and the rights of Data Subjects. 2. Ensure data protection training is provided to all colleagues and provide additional guidance and support as required or requested. 3. Keep records as required by the data protection legislation. 4. Risk assess each breach/incident and log with the ICO, as necessary. 5. Inform the Board of breaches or incidents that are reportable to the ICO. |
| **Senior Information Risk Owner (SIRO)** | The **General Counsel /** **Company Secretary** is responsible for information risk within MHA and advises the Board on the effectiveness of information risk management across the Organisation. The SIRO will -   1. Implement and lead MHA’s Information Governance Risk Assessment and Management processes. 2. Advise the Board on the effectiveness of information risk management across MHA. 3. Receive training as necessary to ensure s/he remains effective in the role as SIRO. |
| **Chief Executive Officer (CEO)** | Overall responsibility for strategic and operational management, including ensuring that MHA’s policies comply with all legal, statutory, and good practice guidance requirements. |

1. Training and Monitoring
   1. All colleagues must complete the following within three months of commencement of employment and annually thereafter, achieving a “pass” grade:
   * Confidentiality and Information Handling, and
   * Cyber Security Awareness
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk).
3. Resources
   1. MHA policy documents, procedures, and guidance:
   * Mental capacity and deprivation of liberty safeguards policy
   * Nominated Individuals form
   * Computer Use Policy
   * Privacy Notice - Colleagues
   * Privacy Notice - Residents and Tenants
   * Privacy Notice - MHA Communities
   * Privacy Notice - Relatives
   * Privacy Notice - Supporters
   * Privacy Notice - Sales and Letting
   * Privacy Notice - Website
   * Privacy Notice - MHA Mobile App
   * Disclosure receipt - Data Subject
   * Disclosure receipt - Police
   * Disclosure receipt - Safeguarding
   * Disclosure receipt – Coroner
   1. External Resources
   * [The Data Protection Act](https://www.gov.uk/data-protection)
   * [The Privacy and Electronic Communications (EC Directive) Regulations 2003](https://www.legislation.gov.uk/uksi/2003/2426)
4. Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Version Date | Revision Description / Summary of Changes | Author | Next Review Date |
| 9 | July 2024 | Compliance review and updated policy, recoded to IG03 | Data Protection Officer  Head of Standards and Policy | July 2027 |